Roman Chmilewsky

Enhancing Implementation Process of UTM Appliances through Automation

Helsinki Metropolia University of Applied Sciences

Master's Degree

Information Technology

Master's Thesis

1 December 2017

Helsinki Metropolia University of Applied Sciences

Preface

I started my Master Thesis three years ago, and I must confess that I wouldn't have been able to complete this study without the support of my family, academic community and colleagues at work.

In this regard, I would like to express my gratitude and respect to my excellent supervisor, Mr Ville Jääskeläinen, for his readiness to guide and support me during the research process. I am grateful to him for his patience, understanding of students' needs and his enthusiastic attitude towards his work.

I would also wish to express my deep appreciation to Ms Zinaida Grabovskaia, who introduced me to the discipline of academic writing in an exciting and comprehensive manner. I especially value her talent to encourage students in their academic endeavours towards the completion of their Master's Thesis.

I am also very grateful to Mr Thomas Rohweder for his extraordinary ability to make complicated issues easy to understand and ensure that all his students are aware of how to structure their research.

As for my colleagues at work, I would like to say a big thank you to the Director of Corporate Project Management, Service Delivery & Operations of the case company for his support during the application process and his readiness to help with the final proposal of this study.

Obviously, I would like to thank my family members for their everlasting patience, kind understanding and great psychological support.

Roman Chmilewsky
1 December, Helsinki

Author Title Number of Pages Date	Roman Chmilewsky Enhancing Implementation Process of UTM Appliances through Automation 60 pages + 4 appendices 1 December 2017
Degree	Master's Degree
Degree Programme	Degree Programme in Information Technology
Instructors	Ville Jääskeläinen, Principal Lecturer

This Master's Thesis analyzed existing implementation practices of Fortinet UTM (Unified Threat Management) firewalls of the case company and determined the pitfalls that might lead to considerable delays with deliveries, incorrect configuration and degraded performance of UTM firewalls within customers' corporate networks. Based on these findings, the current study also aimed to provide concise guidelines on how to minimize the risk of security breaches within corporate networks of the case company customers while implementing and maintaining UTM security appliances. This is especially topical, because even though Fortinet UTM is a very versatile security system which can provide reliable security shield for any corporate network, there is a considerable amount of cases when UTM firewalls either have not been configured correctly or implemented outside the SLA.

Thus, the objective of this Thesis was to identify strengths and weaknesses in implementation process of Fortinet UTM security gateways of the case company. Furthermore, the current study offered practical recommendations for the Service Production management team concerning improvements in the implementation process of UTM devices within customers' corporate networks.

To meet the objectives, the Thesis starts with the analysis of the current state of the case company, which is followed by the first round of data collection. It continues with the analysis of the existing literature concerning service improvement techniques that focuses on the most comprehensive practices of UTM implementation. Moreover, the literature sources are analyzed on micro level to identify the tools that can be used to tackle the challenges defined in the current state analysis. This allowed to create a conceptual framework for this study.

After generating the conceptual framework, the second round of data collection was carried out to reconfirm the results of the first round of data collection. This helped to develop a provisional proposal of this research. As soon as the provisional proposal was generated, it was presented for the attention of the internal stakeholder. This allowed to conduct the third round of data collection and eventually create the final proposal of this research.

Concerning the outcome, this Thesis aimed to create practical recommendations for the Service Production Management team for enhancing implementation process of UTM devices within customers' corporate networks through automation which encompasses standardized and enhanced configuration and maintenance practices.

Keywords	IT Automation, ITIL CSI, Networking Security, UTM

Contents

Preface
Abstract
Table of Contents
List of Figures
List of Tables
Acronyms

1 Introduction 1

1.1 Case Company Background 1
1.2 Business Challenge 4
1.3 Research Objective 5
1.4 Scope and Structure of Study 5

2 Methods and Materials 7

2.1 Research Approach 7
2.2 Research Design and Process 9
2.3 Data Collection and Analysis Methods 10
2.3.1 One-to-One Interviews 12
2.3.2 Web-based Questionnaire 12
2.3.3 Statistics from Efecte 13
2.3.4 Personal Observation 13
2.3.5 Focus Group 14
2.3.6 Interview with External Expert 14
2.3.7 Interview with Internal Stakeholder 14
2.4 Validity and Reliability Plan 14

3 Current State Analysis 17

3.1 ITSM Practices of Case Company 17
3.2 Implementation Process of UTM Appliances in Case Company 19
3.3 Objectives of Implementation Process of UTM Appliances 21
3.4 Current Status of Implementation Process of UTM Appliances 22
3.4.1 Common Efecte Statistics 22
3.4.2 Splunk Statistics and Trends 23
3.4.3 Findings from Interviews and Web-based Questionnaire 24
3.4.4 Feedback from Other Departments of the Case Company 27

3.4.5 Benchmarks from External Expert 27
3.4.6 Results of Interview with Company's Internal Stakeholder 27
3.4.7 Results of Personal Observation 28
3.5 Strengths 29
3.6 Weaknesses 30
3.7 Key Challenges 33

4 Best Practices of Service Improvement 35

4.1 CobIT Framework 35
4.2 PRINCE2 Framework 37
4.3 ITIL Continual Service Improvement 39
4.4 Automation as Main Driving Force of ITIL CSI 41
4.5 Pros and Cons of IT Automation 42
4.6 Future of IT Automation 43
4.7 Conceptual Framework 43

5 Generating Proposal 47

5.1 Validation of Proposal 50
5.2 Final Proposal 52

6 Discussion and Conclusions 54

6.1 Summary 54
6.2 Managerial Implications 56
6.3 Evaluation of Validity and Reliability 57
6.4 Further Development 58

References

Appendices
Appendix 1. One-to-one Interview
Appendix 2. Web-based Questionnaire
Appendix 3. Focus Group
Appendix 4. Interview with External Expert

List of Figures

Figure 1. Service Portfolio of the case company ……..10
Figure 2. Action-Reflection Cycle ……....15
Figure 3. Research Design ……..……..…16
Figure 4. The ITIL Service Lifecycle ……....24
Figure 5. UTM Implementation Process: Teams and Responsibilities ……...26
Figure 6. Sequence of Processing Delivery Ticket ……....27
Figure 7. Efecte Implementation Process of Security Gateways ……..…29
Figure 8. Splunk - Implementation Process of Security Gateways ……..…30
Figure 9. Ringelmann Effect ……...…34
Figure 10. Inactive UTM licensing ……..…..37
Figure 11. Correctly and incorrectly registered UTM appliances ……..…38
Figure 12. CobIT Focus Areas ……...…42
Figure 13. PRINCE2 Principles ……...…..43
Figure 14. PDCA Cycle ……...……45
Figure 15. The seven-step improvement process ……..…46
Figure 16. Conceptual Framework ……...…50
Figure 17. Logical Scheme of the Provisional Proposal ……53

List of Tables

Table 1. Data Collection Techniques ……....18
Table 2. Key Challenges of the Implementation Process of UTM Appliances ……..….39
Table 3. Automation Drivers and Associated Action Points ……..…51
Table 4. Provisional Proposal ……...….54
Table 5. Final Proposal ……...……57
Table 6. Managerial Implications ……..……61

Acronyms

AR	Action Research
CSA	Current State Analysis
DM	Delivery Management
ENS	Enterprise Network Solutions
IPS	Intrusion Protection System
ITIL	Information Technology Infrastructure Library
ITSM	Information Technology Service Management
POC	Point of Contact
SD	Service Desk
SLA	Service Level Agreement
SLO	Service Level Objective
SO	Service Operations
SS	Service Strategy
SSL	Secure Socket Layer
ST	Service Transition
UTM	Unified Threat Management
VPN	Virtual Public Network
WLAN	Wireless Local Area Network

1 Introduction

In modern world where any company is a subject to constantly emerging and rapidly evolving on-line security threats, implementation and maintenance of cost-effective data security policies play a pivotal role in running successful business.

Taking into account the current situation in global economy and the fact that companies ruthlessly fight for their place under the sun, reliable protection of networking resources is a corner stone of the existence of any company. In this regard, UTM - Unified Threat Management system serves as a versatile tool for addressing security related issues of any company, irrespective whether it is a small, medium or large business.

As Tam (2013:20) suggests the Unified Threat Management system ”solves three critical needs: The need of better security, the need of more efficient security … and the need of having cost effectiveness”. He further states that a single UTM device can provide a comprehensive set of security features, e.g. AntiSpam, AntiVirus, Web Filtering, etc. without compromising the performance and with the same quality as if separate dedicated devices were used. This also allows any company to securely operate on-line and consequently maintain its competitive advantage on the market.

Therefore, it is of crucial importance to enhance the implementation process of UTM appliances producing practical recommendations for the managerial team of the case company on how to achieve it.

1.1 Case Company Background

The case company is one of the leading Finnish corporations in telecommunications. It provides cost-effective, easy to deploy, secure and high-quality communication and networking services to corporate clients in Finland and abroad. In addition, the case company offers diverse telecommunication services to consumers, facilitating communication, security and entertainment.

Due to the acquisition of two companies in 2014, the case company became truly global. With its headquarters in Helsinki, it operates in the Eastern and Western European telecom markets.

The service model of the case company complies with the best practices of ITILv3 and it is harmonically incorporated into the business processes of its customers to ensure an effective delivery of services and professional management of business projects. The Service Desk of the case company serves as the first point of contact for customers' IT teams and Help Desks when they need to report about incidents or make service requests related to their networking infrastructure.

Even though the case company incorporates multiple departments, the driving forces of its successful business are the Service Production and Sales departments. In its turn the Service Production Department consists of the Service Desk team, Enterprise Network Solutions team and Project Management team.

To maintain competitive advantage on the market, the case company continually enhances its values, mission, vision and strategy.

The values of the case company serve as a basis for the company's growth and constant development. They can be expressed in an abbreviated form as 'FSB', where: 'F' stands for 'Fast' and means that customers of the case company obtain required services in a quick and efficient manner; 'S' stands for 'Straightforward' and means that the case company delivers its services in an easy to comprehend manner and implement them eliminating complex and expensive solutions; 'B' stands for 'Bold' and means that the customers of the case company must be always positively surprised with original advertising, interesting offers and opportunities of using new products and services.

In regards to the mission and vision, the case company thrives to provide excellent customer service experience in order to have the most satisfied customers, which eventually ensures acquiring of new contracts and safeguarding the existing ones.

As for the strategy of the case company, it has customer centricity in its core and aims to achieve four major goals. First of all, to satisfy both consumer and corporate clients by providing excellent services and proactively adapting to their future needs. Secondly, to ensure financial growth by investing into development of innovative and cost-effective services. Thirdly, to ensure fast market growth by expanding company's service portfolio and forming partnership with profitable and fast growing companies. Lastly, to become one of the most desired employers in Finland by investing into education

and professional development of their employees. This consequently allows the case company to have certified specialists whose knowledge and skills are internationally recognised and whose work ensures that the services of the case company are implemented and supported at the highest level.

The service portfolio of the case company includes numerous cost-effective and operator-independent services that are targeted at individual consumers and corporate clients. With the help of the case company services its corporate customers can enhance their business in such areas as Data Security Services, Network Management and Monitoring Services, Hosting Services, Secure Access and Networking Services, Industrial Internet, Social Communication, etc. In percentage equivalent, all the services of the case company can be presented as illustrated in Figure 1 (Case Company 2017).

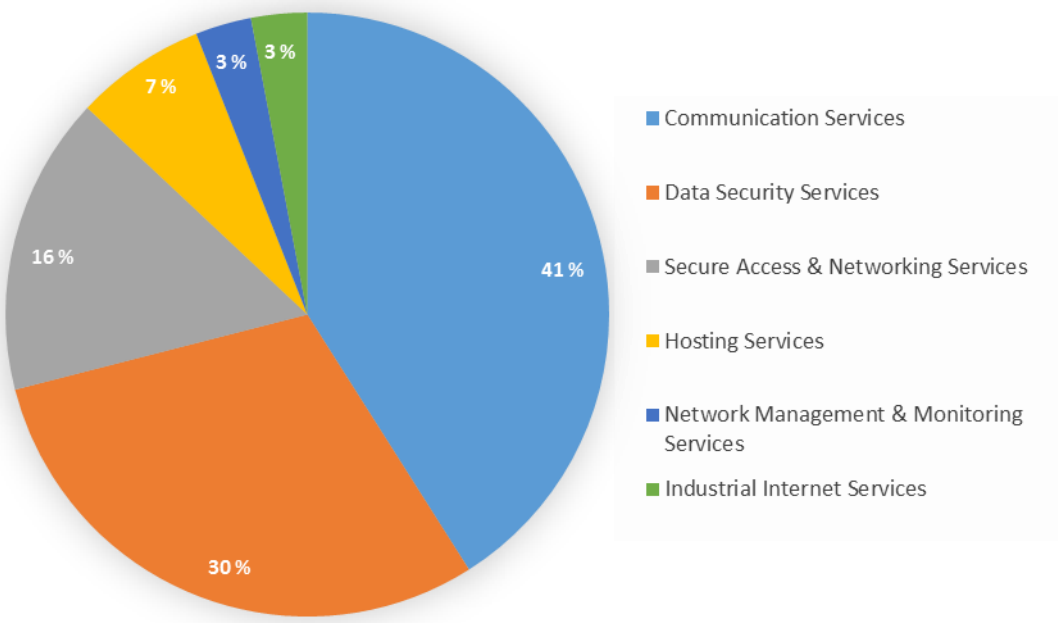


Figure 1. Service Portfolio of the case company (Case Company 2017).

As seen in Figure 1, one of the mostly developed and widely provided services to corporate clients by the case company are Data Security Services that comprise 30% of the total amount of all the services.

Data Security Services are implemented with the help of the 3rd party hardware products and their accompanying services. The scope of the products and associated services is very wide depending on the specific customer requirements, it comprises CRYPTOCard tokens from Gemalto N.V. (former SafeNet, Inc.), SSL VPN appliances from Juniper Networks, WLAN Controller and Access Points from Aruba / Hewlett Packard (former Aruba Networks), Secure E-mail Gateways from F-Secure Corporation, Enterprise Firewalls from Fortinet, Inc., etc.

Taking into account that Fortinet enterprise firewalls and their associated services are the main product from 'Data Security Services' of the case company, they determine the scope of the current study, its business challenge and research objectives.

1.2 Business Challenge

Even though Fortinet UTM is a very versatile security system which can provide reliable security shield for any enterprise network, there has been a considerable number of cases when UTM appliances either have not been implemented correctly or implemented with considerable delays.

Nowadays, successful implementation of Security Gateways empowered by UTM capabilities within customer' networking environment has become one of the top priorities of the case company. It is because existing implementation practices of Fortinet firewalls very often lead to lengthy installation times, inability of local IT personnel to provide correct information for initial configuration and assist with the installation, and consequently to unsatisfactory experience of customers. Therefore, the aim of this study is to determine strengths and weaknesses in the implementation process of UTM firewalls within networking infrastructure of the case company customers, and to provide practical guidelines for Enterprise Networks Solutions management team on how to improve the installation process and performance of Fortinet FortiGate firewall units according to the best practices of UTM implementation.

1.3 Research Objective

This study aims to generate a proposal for ENS (Enterprise Network Solutions) management team for improving the installation process and performance of Fortinet FortiGate firewalls through the best practices of UTM implementation.

In this regard, the main research question is formulated as follows:

How to enhance the implementation process of UTM appliances of the case company?

To find the answer to the main research question, the following sub-questions were addressed:

1) What factors influence the implementation process of the case company UTM devices?
2) What benchmarks are used by the case company for implementing UTM firewalls?

In addition, the best practices of initial configuration and further maintenance of FortiGate firewalls were analysed in order to have precise understanding about the concepts that can be adapted for eliminating weaknesses in the implementation process of UTM firewalls and consequently for improving their operative performance.

1.4 Scope and Structure of Study

The scope of the study conforms to the necessity of identifying the factors that have positive and negative impact on the implementation process of the case company security gateways and their further operative performance. The study focuses on the best practices of UTM implementation that can be adapted and applied to improve the performance of UTM firewalls in the networking infrastructure of the case company customers.

The study consists of seven sections, where Section 1 introduces the reader to the business challenges and research objectives of the study.

Section 2 defines the *methods and materials* used in the current study. In addition, it provides a comprehensive description of the research design and process; data collection techniques; methods of data analysis and its validation.

Section 3 incorporates *current state analysis* which provides an overview of the current implementation process of UTM appliances, its main objectives, its pros and cons, and related benchmarks of ITIL framework that are used in the case company. This section also represents a detailed list of challenges that require urgent attention in order to improve the implementation process of UTM appliances within customers' networking infrastructure.

Then, Section 4 provides analysis of the most popular business frameworks for service improvement by distinguishing their main concepts on a macro level and identifying on a micro level what approaches can be used to solve business challenge of the current research. Hereby, this section forms the Conceptual Framework of the whole research process.

At last, Section 5 delivers a provisional proposal which was produced based on the previously generated conceptual framework. Further, Section 6 presents the final proposal and Section 7 encompasses conclusions, analysis of the research reliability and validity, managerial implications and potential scenarios of further improvement of the implementation process of UTM appliances.

2 Methods and Materials

This section describes the research approach, the research design and implementation, and related data processing methods and techniques.

2.1 Research Approach

Taking into account the research objective of the current study, the research was carried out employing the Action Research approach, defined by McNiff and Whitehead (2011) as:

> ... a form of enquiry that enables practitioners in every job and walk of life to investigate and evaluate their work. They ask, 'What am I doing? Do I need to improve anything? If so, what? How do I improve it? Why should I improve it?' They produce their accounts of practice to show: (1) how they are trying to improve what they are doing, which involves first thinking about and learning how to do it better; and (2) how they try to influence others to do the same thing. These accounts stand as their own practical theories of practice, from which others can learn if they wish. (McNiff and Whitehead 2011:5)

To be more specific, Action Research was chosen because of the business environment where the author works as a technical service specialist, which allowed him to observe the whole implementation process from the inside by taking direct part in configuring, delivering, installing and maintaining FortiGate UTM firewalls, and form outside by directly communicating to the customers and obtaining their feedback about the quality of 'Data Security Services' of the case company.

Such unique set of responsibilities made it possible to comply with two mainstream approaches of action research, where supporters of one approach state that AR can be profoundly carried out only by an external investigator who will 'watch and report on what other practitioners are doing'; and supporters of an alternative approach think that practitioners themselves are able to justify what they are doing (McNiff and Whitehead 2011: 6). Thus, AR of the first type is known as an interpretive action research and the other one is referred as either self-study or first-person, or simply living action research.

Irrespective of how Action Research is approached to, it gives an excellent opportunity to define a research problem; to utilise different ways of completing all the necessary tasks related to the objectives of the research; to verify with colleagues and customers the effectiveness of the actions and proposals; and based on the analysis of the collected data to implement different new approach of solving research problem which can be more effective than the previous solutions.

Hence, the consecutive and continual chain of observation, reflection, action, evaluation, modification and implementation of a new solution is referred to as an 'action-reflection' cycle, shown in Figure 2 below (McNiff 1988: 9).

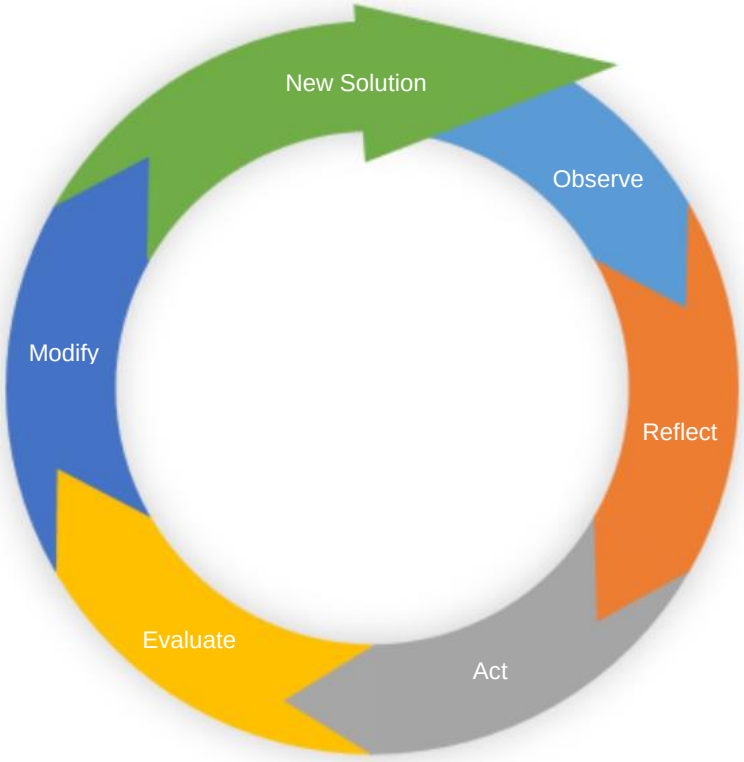


Figure 2. Action-Reflection Cycle (McNiff 1988: 9).

As illustrated in Figure 2, the action-reflection process is continuous. It is due to the fact that as soon as a certain solution is found at a particular point of the research, that point can introduce a new challenge which may require the researcher to reiterate the whole cycle until the most suitable solution to the problem is found (McNiff and Whitehead 2011: 10).

Taking into account that AR can include all types of data gathering methods (Coughlan and Coghlan 2002: 225), this research was equipped with such data collection tools as personal observation, interviews, on-line questionnaire and focus groups, and statistics from the ITSM system called Efecte.

2.2 Research Design and Process

In order to successfully complete any task, it is obligatory to identify its objectives and all the necessary actions that must be taken in order to achieve them. This is especially true with any research or investigation, because only precise understanding of the research components and necessary actions can guarantee its effective accomplishment. Thus, research design and related processes are shown in Figure 3 below.

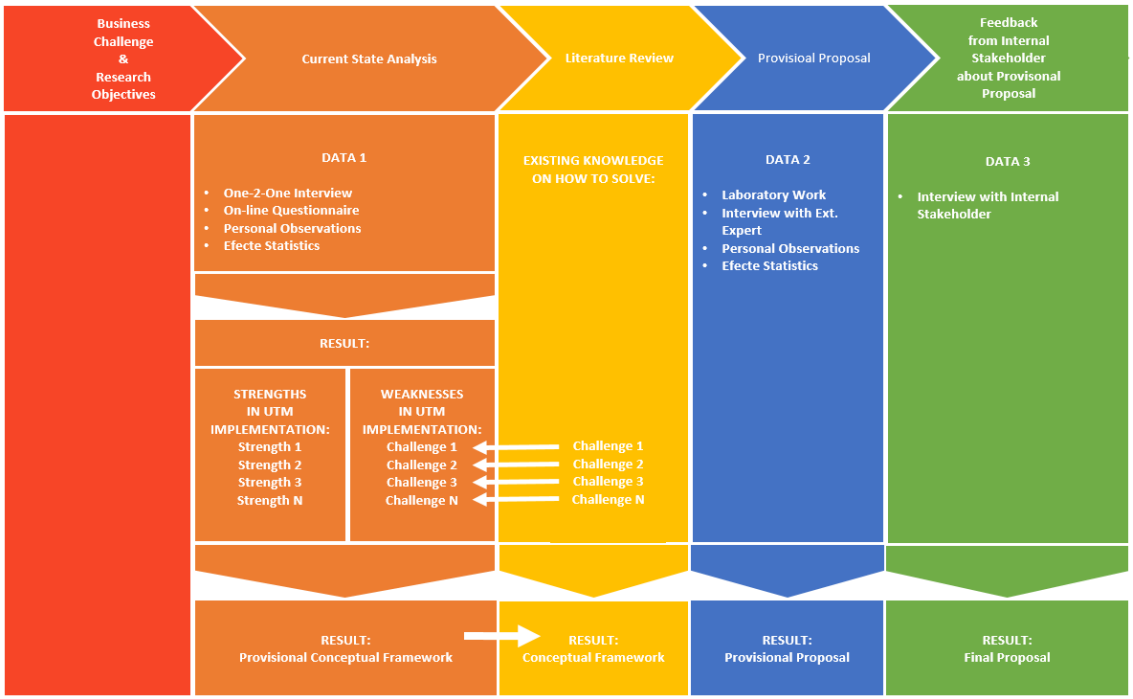


Figure 3. Research Design.

As illustrated in Figure 3, the current study commences with determining the business challenges and associated research objectives. After that, the first round of data collection was conducted to identify the strengths and weaknesses in implementing and maintaining UTM security appliances in the corporate networks of the case company customers. Therefore, it contributed to generating a CSA - Current State Analysis. As soon as the CSA was completed, Conceptual Framework was generated by evaluating

the most recognised literature sources related to enhancing the implementation process of UTM appliances on a macro level. The aim of this evaluation was to determine the existing processes of UTM implementation and benchmarks related to the challenges highlighted in the CSA on a micro level.

Then, in order to validate the previous data, the second round of data collection was conducted, which resulted in generating a provisional proposal about enhancing the implementation process of UTM appliances in corporate networks of the case company customers.

After presenting the provisional proposal to one of the stakeholders of the case company and receiving the feedback, which encompassed the third round of data collection, the final proposal was generated to meet the objectives of the current research.

2.3 Data Collection and Analysis Methods

The study comprises a fusion of the qualitative and quantitative research methods for data collection, because it includes a combination of the statistical data from the ITSM system and data gathered during different types of interviews with ENS engineers, Service Operation Managers and members of other teams about the effectiveness of the implementation process of UTM appliances in the networking infrastructure of the case company customers. Thus, the decision to use different research methods was driven by the research essence and its objectives.

Primarily, *qualitative data* were acquired by utilizing one-to-one interviews conducted to define the factors that may improve the implementation process of UTM appliances. Furthermore*, a web based questionnaire* was employed to define the factors that negatively influence the implementation process of UTM firewalls. Moreover, members of other case company departments were gathered into a *focus group* in order to obtain their opinion about advantages and disadvantages of the implementation process of UTM appliances. In addition, an external IT specialist from another company was invited to share his knowledge about benchmarks related to the research objectives of the current study. The most important interview was carried out with the internal stakeholder of the case company, which was mainly conducted to receive comments about provisional proposal. Last but not least, personal observation was employed to monitor the

implementation process of UTM appliances on a daily basis which contributed to the collection of the qualitative data.

Quantitative data was acquired from the internal ITSM system Efecte which is used to monitor the effectiveness of the implementation process of UTM appliances within the networking environment of the case company customers. In other words, Efecte provides the possibility to generate computerized reports about the ability of the ENS team to meet SLA objectives related to configuring, delivering, installing, testing and maintaining the UTM firewalls. An overview of the data collection methods is shown in Table 1 below.

Table 1. Data Collection Techniques.

Respondents	Method	Date & Duration	Topic / Qs & As
1st Round			
14 ENS Engineers	One-to-One Interviews	18.02.2017 (30 min)	See Appendix 1
14 ENS Engineers	Web-based Questionnaire	25.02.2017(15 min)	See Appendix 2
Researcher	Personal Observation	01.08.2016 – 01.02.2017	
Researcher	Efecte	01.08.2016 – 01.02.2017	
2nd Round			
Head of the Customer Relations Managers, Head of the Service Delivery Managers, Solutions Architect and Customer Relations Manager	Focus Group	08.02.2017 (30 min)	See Appendix 3
External IT Specialist	One-to-One Interview	28.03.2017 (30 min)	See Appendix 4
Researcher	Personal Observation	01.03.2017 – 08.05.2017	
Researcher	Efecte	01.03.2017 – 01.05.2017	
3rd Round			
Stakeholder: Head of the Service Delivery and Operations	Interview	05.05.2017 (30 min)	

Qualitative Data Quantitative Data

As Table 1 demonstrates, the first round of data collection comprises internal sources of the ENS team. The second round of data collection includes information which was obtained from the IT specialist of another company, who is responsible for the imple-

mentation and further maintenance of UTM firewalls. Data acquired from the external expert helped to identify the factors that have influence on the implementation process of UTM appliances in another company and was utilized as a benchmark.

Throughout the second round of data collection, Service Operations managers and managers from other departments of the case company were invited to participate in a web based focus group. This provided a unique opportunity to obtain data about the effectiveness of the implementation process of UTM appliances from the managerial perspective.
During the third round of data collection, an internal stakeholder was asked to review the provisional proposal and share his comments. The various types of collected data are presented in greater detail below.

2.3.1 One-to-One Interviews

During the first round of data collection, one-to-one interviews were conducted with all the members of Enterprise Network Solutions team. Every ENS system engineer was requested to express his opinion on the factors that would speed up the delivery process of the new UTM devices to the customers' sites, simplify their installation and improve their further maintenance and operative performance. It is worth mentioning that all the respondents were enthusiastic to provide answers to the proposed question that are recorded in Appendix 1.

After all the answers were documented, they were analysed and differentiated into the categories in accordance with the various stages of the implementation process of UTM appliances: site survey and planning; initial configuration; delivery; installation and maintenance. After differentiation process, all results of the one-to-one interviews have been identified and recorded.

2.3.2 Web-based Questionnaire

During the first round of data collection a web-based questionnaire was also executed. It consisted of one main question and eight predefined answers, and its main objective was to obtain explicit information from ENS engineers about the aspects that have a negative impact on the implementation process of UTM appliances in customers' net-

working infrastructure. To complete this task, a combination of Google Forms, Google Sheets and Google Analytics were employed. In terms of the questions of the web-based questionnaire, they were formulated in the precise compliance with the main objectives of the case company implementation process of UTM appliances. When ENS engineers received a web link to the questionnaire, they were requested to specify the most common factors that have negative impact on the effectiveness of the implementation process of UTM appliances. The web-based questionnaire also provided the possibility for the engineers to expand their responses by stating other reasons that were not specified in the predefined list of answers. As soon as the web-based questionnaire was completed, Google Analytics performed computation and graphically presented the results, shown in Appendix 2.

2.3.3 Statistics from Efecte

Efecte statistics related to the implementation process of UTM appliances were gathered during the whole study. On a monthly basis, specialized Efecte reports that were designed according to the objectives of the implementation process of UTM appliances, shown in Appendix 3, were monitored and saved as screenshots. Then, all the collected data from Efecte were compared against the predefined objectives of the implementation process of UTM appliances.

2.3.4 Personal Observation

Personal observations were carried out by the researcher by means of communicating with the corporate clients, and configuring, delivering, installing and maintaining UTM firewalls in their networking environment. All the observations related to the current state of the implementation process of UTM appliances were recorded on a daily basis. The researcher's position as a Technical Service Specialist allowed to assess the effectiveness of the implementation process of UTM appliances from the system engineer point of view and from the customers' perspective. Personal observation of the researcher complimented the data which was extracted from Efecte and which was described in the first two rounds of data collection, presented in Table 1 above.

2.3.5 Focus Group

Throughout the second round of data collection, a focus group was organized in order to receive information from the members of other teams that work in co-operation with Enterprise Network Solutions team of the case company. To complete this task Head of the Customer Relations Managers, Head of the Service Delivery Managers, Solutions Architect and Customer Relations Manager were invited to comment on the strengths and weaknesses in the implementation process of UTM appliances. Appendix 3 presents the results of the discussion within the focus group.

2.3.6 Interview with External Expert

The second round of data collection involved an interview with an external expert, who works as an IT Specialist for another company. He was asked to share his experience on how to ensure effective implementation of UTM appliances. Interview with the external expert was specifically conducted to reduce the subjectivity of this study. Results of the interview, shown in Appendix 4, cover all the stages of the implementation process of UTM devices and provide a comprehensive overview of utilized practices in another company to ensure effective configuration, delivery, installation and maintenance of UTM firewalls.

2.3.7 Interview with Internal Stakeholder

During the third round of data collection, an interview with an internal stakeholder of the case company was conducted. This interview was of a great importance, because the internal stakeholder was informed about the outcome of the previous rounds of data collection and was provided with the provisional proposal on how to enhance the implementation process of UTM appliances. During the course of the interview, it was agreed that the proposal would be adjusted according to his comments.

2.4 Validity and Reliability Plan

One of the most common disadvantages of the action research is the possibility that it may become subjective and unreliable to a certain degree, because its results ‘cannot be universally tested (McNiff 1988: 131). Thus, in order to safeguard trustworthiness of

the action research, it is important to meet two necessary criteria of data collection and analysis, namely research validity and reliability.

Generally, *validity* is viewed as a certain degree of accuracy and meticulousness of the research data. During validation process of the research data, researchers must affirm that they evaluated or observed exactly what they were intended to evaluate or observe (Swetnam 2004: 23). Furthermore, data validity have internal characteristics that exhibit whether the research results can be verified by the collected data (Cohen et al. 2000: 107) and external characteristics that describe the extent 'to which the results can be generalized to the wider population, cases or situations' (Cohen et al. 2000: 109). The last but not least factor that researchers have to comply with is the data triangulation, which encompasses data validity and reliability; and utilization of several research methods and data collection techniques (Cohen et al. 200: 112).

Thus, to ensure the validity of the present study, a combination of the qualitative and quantitative research methods were employed. In addition, to safeguard data triangulation, the research data were collected by using different data collection techniques: personal observation, interviews, on-line questionnaires, etc. Moreover, data triangulation was ensured by collecting data from various sources: internal and direct, e.g. ENS system engineers and Service Operations Managers; internal and indirect, e.g. managers of other teams of the case company; external and direct, e.g. customers; and external indirect, e.g. IT specialist from another company.

In regards to research *reliability*, it describes the process of minimising the amount of potential errors and bias (Yin 2003: 37). Strictly speaking, research is acknowledged to be valid only if the level of the research subjectivity is reduced to its minimum. As Swetnam (2004) mentioned, the notion of the research reliability pursues to affirm if 'the same procedures, experiments or actions carried out again produce the same result' (p.23).

In terms of the research reliability, it was assured by the three rounds of data collection that provided all the respondents with the possibility to express their opinion concerning gathered and analysed data, and eventually reassure reliability of the research data. Moreover, the possibility of the research replication was ensured by the rigorous description of the data collection techniques and data analysis methods.

Summarizing all the important characteristics of valid and reliable research it is necessary to comply with the following criteria. First of all, the study needs to employ different research methods. Secondly, research data has to provide the possibility of identifying the scope of the research and meeting its objectives. And lastly, the whole design of the research must supply the means to other scholars and practitioners to replicate it.

3 Current State Analysis

This section evaluates the current practices and tools utilized by the case company for implementing UTM appliances within customers' networking infrastructure. It also identifies the advantages, disadvantages and challenges experienced by the case company in regards to configuration, delivery, installation and maintenance of UTM firewalls. Moreover, this section presents provisional proposals on how to enhance the implementation of UTM appliances through the best practices of the ITIL Continual Service Improvement process.

3.1 ITSM Practices of Case Company

The IT infrastructure of the case company is built in accordance with ITIL – Information Technology Infrastructure Library, which equips the company with solutions and tools that are utilized to plan, transition, operate and improve IT services (ITIL 2012: 6). The choice of the ITIL framework was determined by the fact that it can be effectively incorporated in the dynamically changing environment of any IT company and it encompasses vendor neutral best practices adopted not only from the public frameworks and standards, but also from the proprietary knowledge of organizations and individuals (ITIL 2012: 2).

ITIL was first published in 1992 and since then it has become one of the most widely used sources of the best practices for Service Management because it describes in great detail the entire Service Lifecycle.

Thus, the ITIL framework enables the case company to maintain its operative performance on the global market by effectively managing its own IT resources and resources of its customers, which helps to build strong relationships with the customers and according to the commonly recognised IT (ITIL 2012: 8). In general, ITIL consists of five publications that describe Service Lifecycle presented in Figure 4 below (ITIL 2012: 4).

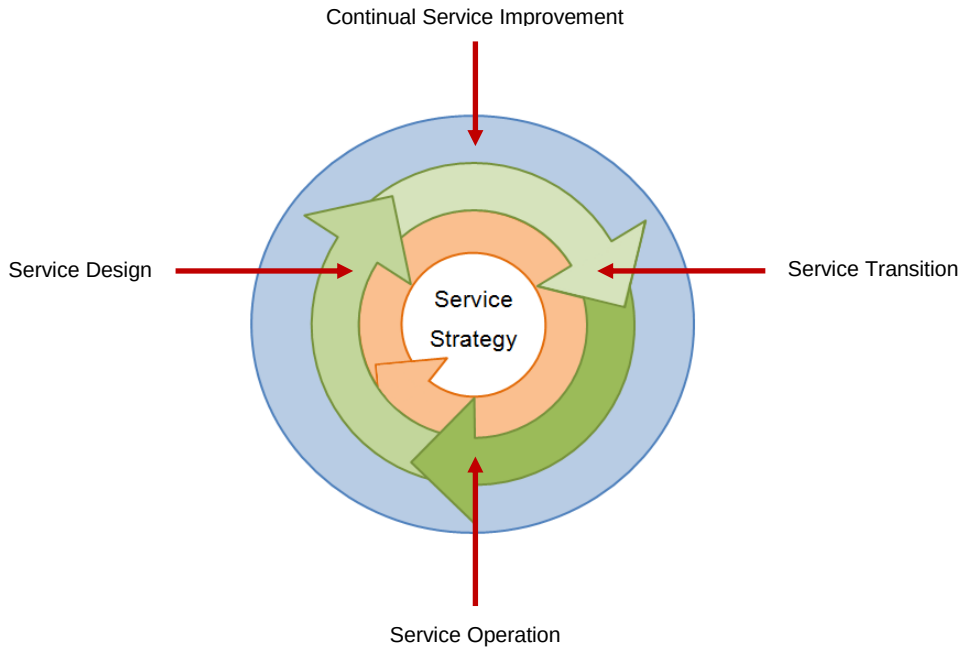


Figure 4. The ITIL Service Lifecycle (ITIL 2012: 4).

As Figure 4 shows, ITIL describes the entire Service Lifecycle, which consists of five stages: SS – Service Strategy, SD – Service Design, ST- Service Transition, SO – Service Operation and CSI – Continual Service Improvement.

The Service Strategy of the case company defines four criteria: *perspective* which identifies the business objectives and provides a clear vision in terms of possible directions of business development; *position* which allows to differentiate the case company from other service providers; *plan* which determines how the case company can achieve its objectives; *pattern* which empowers the case company to adjust its practices and cope with new challenges on the way of achieving its objectives (ITIL 2012: 62).

In terms of the Service Design phase, it enables the case company to transform its service strategy into a plan for delivering service objectives while serving as a guideline for the service design, development and management (ITIL 2012: 80). During ITIL SD phase, service portfolio and assets are identified to address personnel, processes, products and partners of the case company.

In regards to the ITIL Service Transition, it assures that current and new services comply with the business objectives of the case company. It also helps to create the Service Knowledge Management System, which facilitates learning and consequently increases the productivity of the entire lifecycle of the case company services (ITIL 2012: 140).

The management of all the activities, processes and technologies is described by the ITIL Service Operation phase. It ensures the satisfaction of the case company customers through delivering and supporting the required products and related services; minimizing the amount of the potential incidents with the provided services; and ensuring a secure access to the provided services only by authorized personnel (ITIL 2012: 193-194).

Concerning the ITIL Continual Service Improvement phase, it helps to manage ongoing changes within the business environment of the case company by identifying current challenges and implementing required changes in order to improve all the business processes, services and actions. Consequently, ITIL CSI allows the case company to safeguard the entire service lifecycle and maintain competitive advantage on the market (ITIL 2012: 256).

Taking into account the objectives of the current study, the next chapter describes the implementation process of UTM appliances through the most applicable ITIL phases: Service Operation and Continual Service Improvement.

3.2 Implementation Process of UTM Appliances in Case Company

The implementation process of UTM firewalls within the networking environment of the case company customers is aligned with the Service Operation phase of ITIL framework, where responsibilities of the case company personnel are distributed among several teams. To be precise, the Project Management team, which is responsible for co-ordinating the project from its initiation to its completion and ensuring co-operation between Delivery Team and Enterprise Network Solutions Team. Furthermore, the Delivery Management team which is responsible for acquiring information about customers‘ needs and configuration preferences, ordering and purchasing new UTM devices from the vendor, and delivering new devices to the warehouse of the case company. And, Enterprise Network Solutions Team which is responsible for initial configu-

ration, shipment of configured devices to the actual customer's site, installation and further maintenance of the UTM appliances. Thus, the whole chain of the involved parties and corresponding responsibilities of the UTM implementation process is presented in Figure 5 below (Case Company 2017).

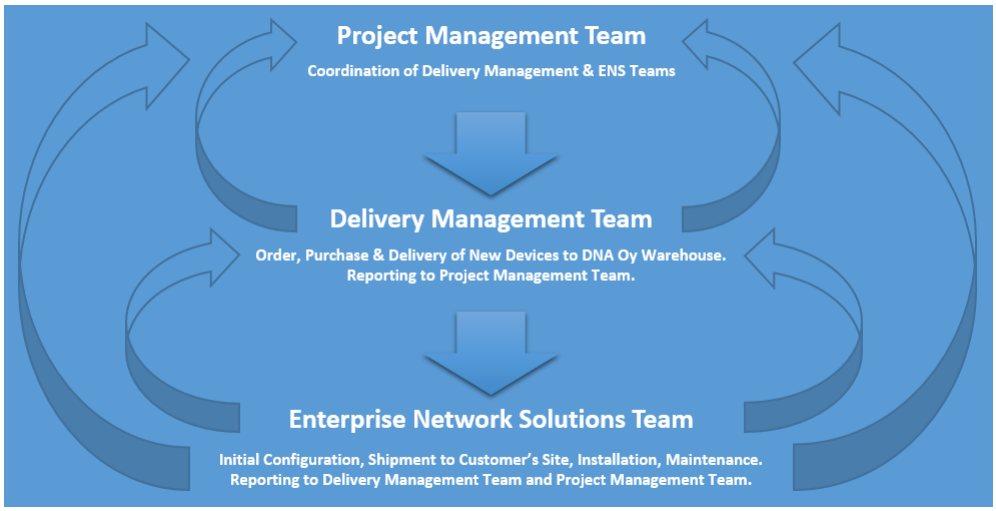


Figure 5. UTM Implementation Process: Teams and Responsibilities (Case Company 2017).

As illustrated in Figure 5, ENS engineers work in close co-operation with Delivery Managers and Project Managers. Every time when a customer of the case company requires to implement a new UTM solution at any particular site, a dedicated Project Manager is assigned to coordinate the whole process. Project Manager creates Delivery Ticket in the case company in-house ITSM system Efecte and assigns to this Delivery Ticket a dedicated Delivery Manager and ENS system engineer. As soon as Delivery Manager ensures that newly purchased UTM device has arrived to the case company warehouse, she or he informs ENS system engineer and reports to Project Manager that new device is ready for configuration. From this moment, effectiveness of the whole implementation process depends on the ENS system engineer, who makes a record about his every single action in the Delivery Ticket.

With the help of the dedicated Delivery Ticket, customers and all the involved parties from the case company may monitor whether any given delivery is processed according to the promised SLA. In its turn, SLA of the delivery defines the objectives of the whole implementation process of UTM appliances within networking infrastructure of

the case company customers, and these objectives are discussed in more detail in the next chapter.

3.3 Objectives of Implementation Process of UTM Appliances

The most important objective of the case company is customer satisfaction. In regard to the implementation process of the case company Security Gateways, this main objective is expressed in ensuring complete functionality of the new UTM appliance at customer's site within twenty one days upon receiving the order from the customer. In order to achieve this objective, Project Manager and Delivery Manager must guarantee, preferably within two weeks, that the new devices have been delivered to the case company premises and that ENS engineer has all the necessary information concerning the initial configuration of the new device. Thus, the ENS system engineer must configure and send the device to the customer's site within the last seven days.

During the whole implementation process, Project Manager, Delivery Manager and ENS engineer must update the status of the Delivery Ticket in Efecte in order to inform peer colleagues about the steps that have been already completed and to ensure that the implementation process of the new firewall is conducted according to the promised time frame. The sequence of the required actions and responsibilities of all the involved parties related to implementing new UTM appliances is presented in Figure 6 below.

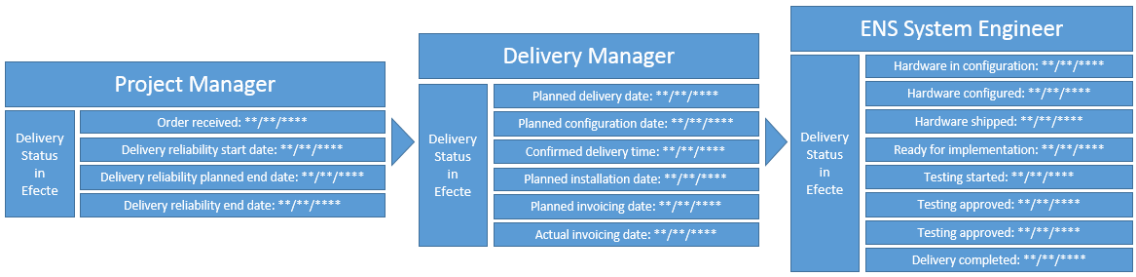


Figure 6. Sequence of Processing Delivery Ticket.

As Figure 6 demonstrates, Project Manager must acknowledge the customer's order by creating a Delivery Ticket and setting the date for completing the project, which is usually 21 days from the date of receiving the customer's request for implementing a new UTM firewall. As soon as general time requirements are identified, Delivery Manager should set more a specific date for configuration, delivery, installation and invoicing.

When specific time requirements are set, the ENS system engineer starts executing the actual implementation process by configuring, shipping and installing new device at the customer's site. During the installation phase, the ENS system must contact the customer at the predefined date and time, guide the customer in a professional and polite manner how to connect the new device to the network and ensure the device is operational by checking whether the customer has access to all the required external and internal online resources. The ENS system engineer must also record all the actions in the Delivery Ticket according to the completed tasks. Upon successful installation of the new device, the Delivery Manager reviews the ticket and sends the invoice to the customer.

In addition to processing the actual delivery, the ENS system engineer must record all the details of the newly installed firewall, e.g. public IP addressing, local IP addressing, management URL, administrative login credentials, etc. in the in-house Efecte database. To finalize the installation, the ENS system engineer must also ensure that the new device is registered in all the monitoring and logging management systems of the case company, and in the online support portal of the vendor – Fortinet. All the instructions that the ENS engineer must follow in order to complete delivery of the UTM appliance in a professional and effective manner can be found in Appendix 1.

3.4 Current Status of Implementation Process of UTM Appliances

The current status of the implementation process of the UTM appliances in the case company can be explicitly demonstrated by the statistics from the in-house ITSM system Efecte and from the operational intelligence platform Splunk.

3.4.1 Common Efecte Statistics

The ITSM system Efecte allows the managerial team of the case company to gather statistics related to every single aspect of Delivery Tickets related to the implementation of the case company UTM appliances. Efecte statistics can be retrieved on a daily, monthly, quarterly and yearly basis. Efecte also permits to differentiate statistics by various criteria, e.g. by Service, Service Group, Service Code, Geographical Location, Delivery Type and Status, Delivery Start and Completion Date, etc. Thus, statistics

related to the implementation process of Security Gateways or in other words, UTM firewalls are presented in Figure 7 below (screen shot from the Efecte system).

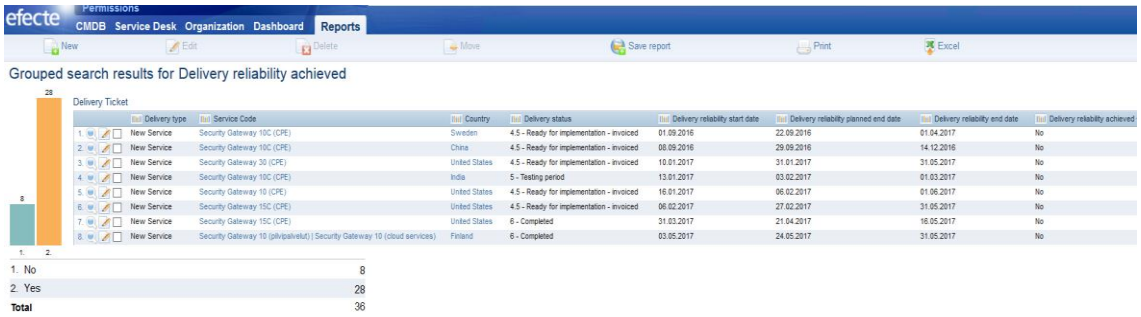


Figure 7. Efecte Implementation Process of Security Gateways.

As Figure 7 illustrates, during one week the ENS team handled thirty six deliveries related to implementing Security Gateway appliances in the networking infrastructure of the case company customers. All of these deliveries are at their final stages. As can be seen, some tickets are in 'Ready for Implementation' phase because new UTM appliances are already configured and sent to the customers' sites; one ticket has 'Testing period' status because new firewalls are already installed and are being tested; and some Delivery Tickets are completed because newly installed Security Gateway appliances successfully went through the testing period and proved to be completely functional. The most important criterion of the presented statistics is 'Delivery Reliability Achieved' value, which vividly demonstrates that out of thirty six Delivery Tickets, eight tickets did not meet the objectives of the case company implementation process. At a first glance, it can be said that the amount of out of SLA tickets is not alarming, but from the perspective of customers, the implementation process of UTM appliances is not conducted to its full potential and consequently does not increase customer satisfaction.

3.4.2 Splunk Statistics and Trends

Another tool, which is widely used in the case company environment for evaluating the implementation process of Security Gateways is a web based platform Splunk. In addition to providing statistics related to the case company processes within a predefined period of time, Splunk allows to identify trends of future development of any given process. Thus, Figure 8 presents statistics from Splunk below.

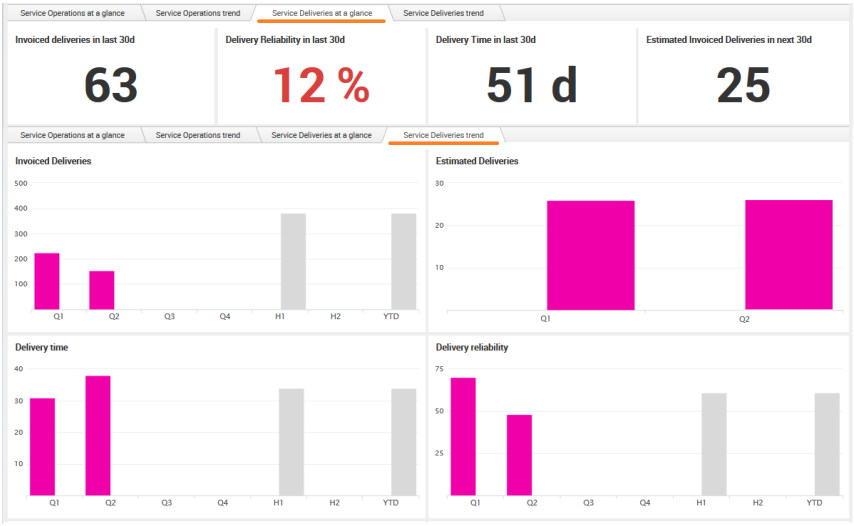


Figure 8. Splunk - Implementation Process of Security Gateways.

As seen in Figure 8, during the last thirty days, the ENS team handled sixty three deliveries of UTM appliances. The average delivery time of the new UTM firewalls was fifty one days, which led to the situation when only twelve percent of deliveries were completed according to the objectives of the implementation process of the case company UTM appliances.

In terms of trends related to the implementation process of Security Gateways, it can be also observed that the number of invoiced deliveries in quarter two considerably decreased, even though the number of deliveries in quarter two remained the same as the number of deliveries in quarter one. Furthermore, in comparison with quarter one the delivery time in quarter two is increased, but the delivery reliability decreased.

Alarming statistics from Splunk demonstrate that the quality of the implementation process of the case company UTM appliances has a tendency for considerable deterioration.

3.4.3 Findings from Interviews and Web-based Questionnaire

Answers of the respondents that were obtained during one-to one interviews and Web-based questionnaire demonstrate that the ENS system engineers considered the lack of information about the required configuration for the new UTM firewalls as one of the

most negative factors that influenced the effectiveness of the whole implementation process of UTM appliances. It is evident that the ENS engineers cannot configure new firewalls and proceed to their shipment if they do not know the customer's requirements. Consequently, it leads to the situations when an ENS system engineer must keep requesting the customer about configuration details and wait for the customer's response for a considerable amount of time. This eventually causes delays and an unsatisfactory experience of all the involved parties.

Another most negative factor was the inability of local IT representatives to assist the ENS system engineer during the installation process either because of inadequate technical background or communication skills. There has been situations when it has been necessary to perform changes on the local ISP equipment in order to ensure that the newly installed UTM firewall can access the Internet, but the local IT person either did not have login credentials to the local ISP router or did not know whom to contact from the ISP side for any further assistance. Moreover, local IT representatives might not have been aware how to connect new firewall within their local network or how to provide the ENS engineer with the possibility to access firewall remotely via FortiExplorer and TeamViewer in case if any changes to the initial configuration were required. Thus, the inability of the local IT personnel to assist the case company system engineer during the installation phase has caused considerable delays and poor customer service experience.

Missing, incomplete or incorrect shipping address and contact details of the local IT personnel was considered to be the third most negative factor that has caused delays with the installation, testing and completion of the delivery. In addition to situations where the customers or Delivery Managers fail to provide required shipping details, there has been situations when customers make an order for the delivery of a new UTM cluster unit to the company's site, which does not have electricity and communication infrastructure. In these cases, customers have redirected new firewalls to the alternative locations, which means that the ENS engineers must reconfigure the same firewalls for the second time to meet the requirements of the new networking environment. As a result, the ENS engineer has not completed the related Delivery Ticket according to the objective of the UTM implementation process.

The next most negative factor of the implementation process of the new UTM appliances was miscommunication between customers and Delivery Managers who tend to

make installation appointments without considering the time difference between a certain location and Finland. This miscommunication has caused situations when the ENS system engineers must assist with the installation of the new firewalls either during the night or early in the morning, e.g. three or four o'clock. It is obvious that the productivity of the person who has spent the whole working day and who should continue performing during the night is considerably less than the productivity of a person who had a good rest. Thus, sometimes mistakes can occur during the installation process that lead to lengthy troubleshooting sessions and repetitive installations.

The fifth most negative factor was the customer's tendency to request configuration changes that are not relevant to the actual installation process of the new UTM appliance. According to the SLA agreement, during the installation phase, the ENS engineer must ensure that 'Primary' and 'Secondary' units of the new firewall successfully form a cluster; local users have access to the internal corporate resources via IPSec VPN tunnel and protected by UTM filters access to the Internet. Despite the fact that some customers are well aware about the mutual agreement between their company and the case company, they are trying to solve all their networking and security challenges during one installation process. Taking into account that installation process is a complex task, customers' additional requests delay installation, testing, completion and eventually invoicing of the related Delivery Ticket.

The ENS system engineers do not consider missing information about local networking infrastructure as the most negative, even though it might introduce some delays, because missing information about the local site can be recovered from the local IT person during the actual installation process.

It is necessary to mention that despite the fact that missing UTM licenses and Efecte device cards can cause delays in finalizing related delivery tickets, the ENS engineers considered these factors as the least negative. Most probably because ENS members can enable UTM licenses themselves without asking for assistance from Delivery Managers. As for recording information about a newly installed firewall in an Efecte devices card, the ENS engineers can remind the Delivery Manager to create it and complete it even after finalizing the related Delivery Ticket.

3.4.4 Feedback from Other Departments of the Case Company

Generally, representatives of the other case company departments were satisfied with the current status of the implementation process of UTM appliances. Nevertheless, occasionally they tend to express their concern about achieved 'Delivery Reliability' related to certain Delivery Tickets. Mostly, it is due to the fact that they are not aware about constraints that ENS system engineers can have during configuration, shipment and installation phases of the UTM implementation process. As demonstrated in Appendix 4, representatives of other departments of the case company considered ENS engineers to be highly skilled professionals equipped with the excellent customer services skills.

3.4.5 Benchmarks from External Expert

In regards to the feedback from the external expert demonstrated in Appendix 4, it was obvious that there is a strong tendency in the company of the external expert to minimize potential mistakes and delays during the configuration and installation phases of UTM appliances. They have tried to achieve this by automating the process of configuration and making installations according to the strict and predetermined requirements. Nevertheless, at the same time, they have provided their customers with flexibility in terms of installation appointments and possibilities to implement new services. Thus, working practices of the external expert can be considered as benchmarks and eventually employed into daily practices of ENS team in order to meet the objectives of the current study.

3.4.6 Results of Interview with Company's Internal Stakeholder

The provisional proposal was completely approved by the internal stakeholder, especially the sections related to *communication templates, networking diagrams, configuration templates* and *installation manuals*. In terms of the *post-installation scripts*, internal stakeholder pointed out that their implementation requires accurate planning because all the actions of the case company must be coordinated with the customers and the vendor. As for the proposal concerning *roles and responsibilities*, the internal stakeholder affirmed that they will be brought for the attention of the Head of the Deliv-

ery Management team. Thus, internal stakeholder requested to perform suggested corrections to the provisional proposal and start generating the final proposal.

3.4.7 Results of Personal Observation

Considering personal observation of the researcher, it can be stated that the whole implementation process of UTM appliances suffers from 'Ringelmann Effect', which was initially discovered in 1913 by Max Ringelmannn. Through practical experimentation, he identified that the efficiency of a certain group of people deteriorates when the number of the group members increases.

Later, 'Ringelmann Effect' was defined by Forsyth (2010: 293) as a tendency when people tend to be less productive when they work with others because of such psychological phenomenon as '*social loafing'.* This phenomenon describes the situations when the members of a certain group gradually loose motivation and reduce personal input towards the common goal because they subliminally count on each other.

As demonstrated in Figure 9, growing number of group members leads to the situations when each member of the group applies less efforts in order to meet common objectives. Consequently, the quality of all the processes within this group gradually decreases.

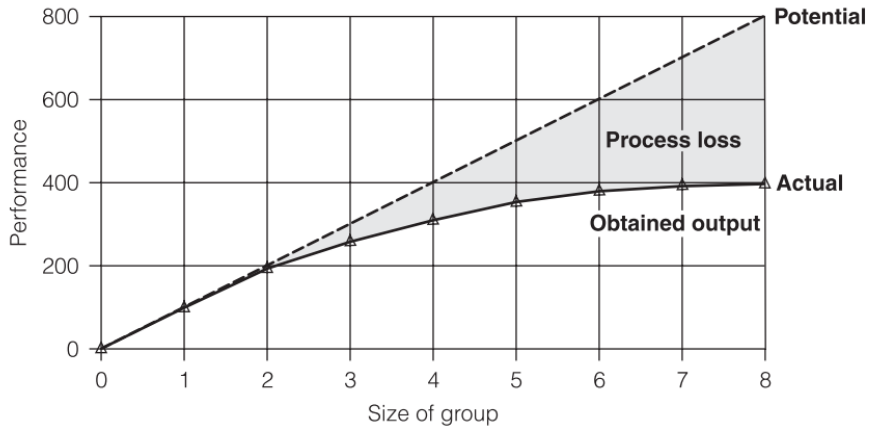


Figure 9. Ringelmann Effect (Forsyth, 2010:294).

This is precisely what is re-occurring in the production team, because the two main factors that stimulate social loafing are explicitly visible in the implementation process

of the UTM appliances. The first factor is an *unidentified personal input*, which can be described as the absence or lack of control over the personal efforts of each team member in regards to completing a common task. The other factor is *free riding*, when certain team members tend to do less in comparison with their peer colleagues, expecting that 'others will make up for their slack' (Forsyth 2010: 296).

To be more precise, Delivery Managers rely on the ENS engineers in obtaining all the necessary technical information concerning required configuration and activating UTM licenses. Whereas, ENS engineers, expect Delivery Managers to complete all the previously mentioned tasks, because it is direct responsibility of Delivery Managers. In their turn, customers hope that Delivery Managers are aware about correct physical address where new units are supposed to be delivered and the ENS engineers already know how to configure new devices even though customers did not provide any site surveys and precise configuration details. On many occasions, customers simply expect the ENS engineers to configure new devices on the fly as soon as they are connected to the Internet line at any given site. This obviously leads to delayed installations and eventually to poor customer service experience, which is also affirmed by the results of one-to-one interviews presented in Appendix 1.

3.5 Strengths

Considering that the case company clients have diverse networking infrastructures and consequently different requirements related to the IP routing, firewall rules, web filtering, etc., the ENS system engineers can satisfy all the technical requirements while implementing UTM appliances in customers' corporate networks. Moreover, due to the extensive expertise the ENS engineers are capable of providing the case company clients with practical suggestions on how to improve the operating performance of the newly installed FortiGate units as well as existing networking devices of other vendors and service providers.

The ENS system engineers can also be proud of their ability to ensure successful implementation of UTM appliances by designing the networking infrastructure for the new clients from the very beginning. It plays a pivotal role in the initial implementation of the new UTM devices and their further operating performance.

The ENS team is also respected by the personnel of other case company departments for their readiness to help in the most challenging situations concerning required hardware that should be purchased, co-ordination of actions with all the involved parties, and operating performance of UTM appliances within corporate network customers.

Thus, according to the personal observation of the author, it can be stated that the key strength of the current implementation process of the case company UTM appliances is the professionalism of the Enterprise Network Solutions team.

3.6 Weaknesses

To clarify how to enhance the implementation process of UTM Security Gateways, it is obligatory to distinguish and perceive all its weaknesses that can be defined as follows.

The first deteriorating factor of the implementation process of UTM appliances was missing or incomplete, or incorrect information about required configuration. This considerably increased the time of the delivery, because ENS system engineer is not aware how a new Fortinet firewall should be configured to meet all the customer's requirements from the technical point of view. Even if ENS system engineer takes an initiative and contacts the customer to retrieve configuration details, there is no guarantee that all the required information is obtained.

Secondly, the inability of the customer or Delivery Manager to communicate to each other and provide correct and complete delivery address and contact details of the recipient considerably increased the time of the delivery. In addition, lack of information concerning deliveries outside European Union, also caused some delays. It is because UTM appliance which is sent without correct supplementary documents recognised by the officials of a certain country can be held at the customs until all the details are clarified.

Thirdly, the inability of customer's local IT personnel providing information about the existing networking infrastructure and to assist with the most basic tasks during the installation process, for example connecting FortiGate device to the local switch, caused inappropriately long installation times. In certain cases, the ENS system engineers needed to reschedule the installation of the new unit for the following day.

The most disturbing weakness of the implementation process of UTM appliances was the absence of the automation process during the initial configuration phase. In other words, the ENS engineers tend to configure every new device from the scratch even though some aspects of firewall configuration are identical across different platforms and customers.

The customer's additional configuration requests that are not related to the initial installation of the UTM appliance also caused extended installation times and consequently poor customer server experience.

Moreover, installation appointments that are scheduled outside the normal working hours of the ENS team also contributed to the number of the installations that needed to be rescheduled for an alternative date and time.

Furthermore, missing UTM licenses that are being ordered only after the initial installation of UTM firewall do not create positive customer service experience, because newly installed firewall without UTM licenses works only as a router and not as a security gateway, which protects users from viruses, intrusion attacks, etc. Additionally, the delivery of the firewall, which was installed but not fully functional cannot be completed until all the UTM licenses are activated. As seen in Figure 10, neither of the UTM licenses were not active on this newly installed firewall.

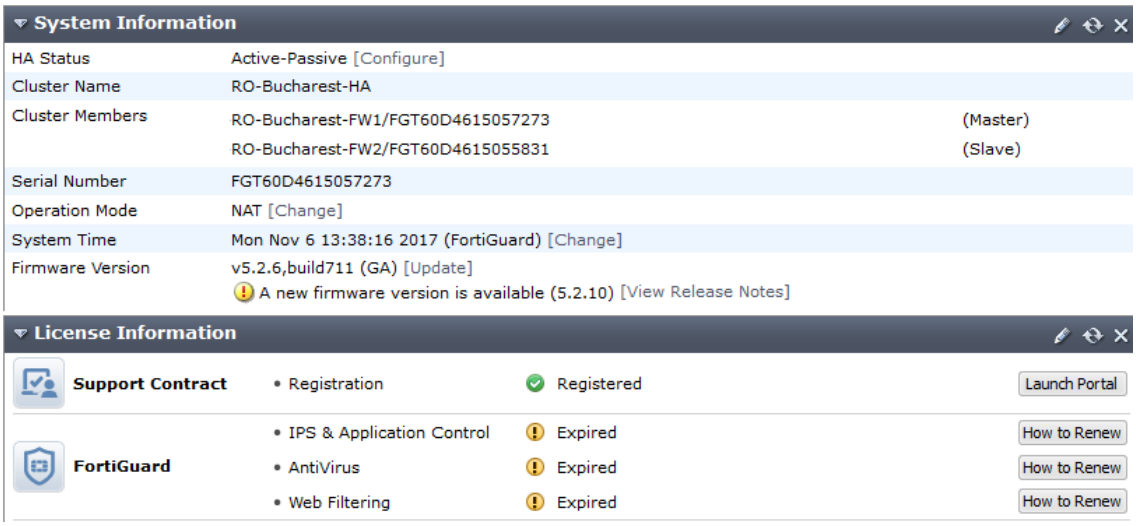


Figure 10. Inactive UTM licensing.

Another factor of the implementation process, which did not look to be important from the first sight, was a missing Efecte device card from the dedicated delivery ticket. This lead to situations when new UTM firewall was installed but not registered in the internal database of the case company. Thus, only a dedicated ENS engineer is aware about the existence of the new firewall. Consequently, the rest of the ENS team does not know via what management IP or URL newly installed device can be accessed and what login credentials should be used. It might not cause an immediate problem, until customer requests changes or report about incident related to the newly installed device. Figure 11 below, vividly demonstrates the difference between correctly and incorrectly registered devices in the Efecte database.

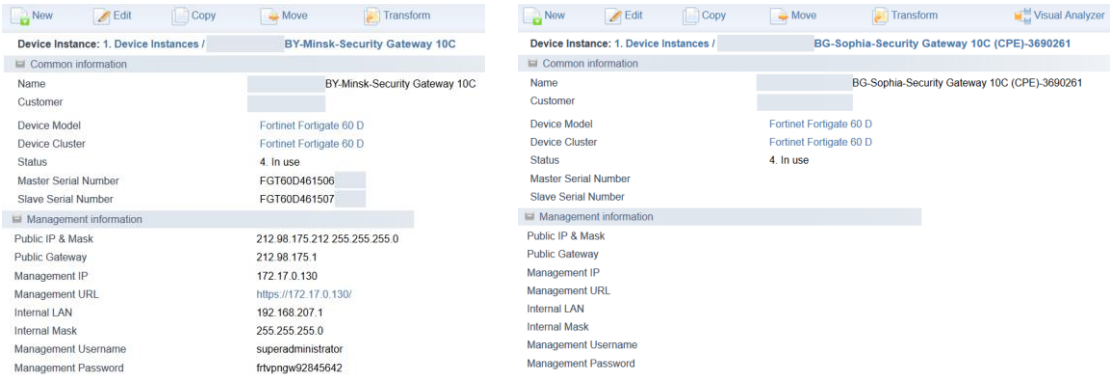


Figure 11. Correctly and incorrectly registered UTM appliances.

The last, but not least weakness of the implementation process of Fortinet Security Gateways was the presence of ‘Ringelmann Effect’, which caused considerable delays with the installation of new UTM devices. It is due to the lack of strict differentiation of the responsibilities among all the parties that are involved in the implementation process. Thus, customer relies on the case company project manager that he or she already knows where to deliver the devices; project managers relies on ENS engineer that he will contact the customer and clarify all the configuration details; ENS engineers rely on the customer and project manager that they will provide all the information concerning configuration and shipment.

Summing up all the weaknesses in the implementation process of the case company UTM appliances, it is apparent that there were three major factors that increase installation times and consequently did not allow ENS system engineers to meet their SLA objectives, they were: poor information flow, absence of automation processes, and ‘Ringelmann Effect’.

3.7 Key Challenges

Taking into consideration all the acquired data, it can be stated that the main challenges that must be tackled to enhance the implementation process of the case company UTM appliances correspond to the delivery reliability of SLA factor which comprises initial configuration, shipment and installation phases; and to imprecisely distinguished responsibilities of all the involved parties of the case company.

If one inspects all these challenges more closely, they can be defined and summarized as shown in Table 2 below.

Table 2. Key Challenges of the Implementation Process of UTM Appliances.

CHALLENGE 1: Initial Configuration	
A	Considerable amount of delivery tickets do not contain correct and concise information about required configuration for the new UTM appliances.
B	Considerable amount of delivery tickets do not contain information about customer's existing networking infrastructure where new UTM firewall is supposed to be installed.
C	Initial configuration of the new UTM devices is not automated.
D	Not all delivery tickets have associated device card.
CHALLENGE 2: Shipment	
A	Some delivery tickets do not have correct and complete recipient details (mobile number and e-mail address) and physical delivery address where a new UTM unit should be shipped to.
B	Not all ENS engineers know what supplementary documents have to be submitted for the attention of the customs while delivering devices outside European Union, especially to such challenging destinations as China, India, Malaysia, etc.
CHALLENGE 3: Installation	
A	Customer's local IT personnel is not able to assist with the most basic technical tasks during the installation.

B	Some of the installation appointments are not scheduled within normal working hours of ENS engineers and some of these appointments overlap with already existing ones.
C	Customers request to perform extra tasks that are not related to the initial installation of the UTM appliance.
D	Considerable amount of newly installed firewalls do not have activated UTM licenses.
CHALLENGE 4: Responsibilities	
A	Some delivery managers tend to ignore their direct responsibilities by allocating certain tasks, e.g. obtaining information about shipment details or required configuration to ENS engineers.

As Table 2 reveals, challenges related to shipment and responsibilities are quite common for any other company. As for the challenges associated with the initial configuration and installation phases, they are specifically acute to the case company due to its nature of business. Nevertheless, irrespective whether it is a common challenge or a specific one, it is necessary to compose a theoretical background in order to comprehend them and eventually eliminate them in practice. Hence, the next section of this research is dedicated to the existing theoretical knowledge concerning possible solutions that can be adopted to cope with the challenges of the case company implementation process of UTM appliances.

4 Best Practices of Service Improvement

This chapter examines existing literature sources dedicated to theories on service improvement in production environment. It commences with outlining leading theories concerning service improvement, gradually advancing to peculiar differences of these theories and consequently, distinguishing the drivers that can be utilized to deal with the challenges of the current research. As a result, this chapter also presents the Conceptual Framework of the whole research based on the analyzed literature sources.
There is no doubt that any company must continuously improve its services to succeed and maintain competitive advantage in the modern business environment. It can be achieved by employing various practices and business frameworks that provide detailed description of all the IT processes and offer solutions on how to overcome potential challenges. Some of the most widely used business frameworks and practices are as follows: CobIT5, PRINCE2, ITIL3, CMMI, SO/IEC 27001, MOF, Agile, Kanban, PMI, etc.

4.1 CobIT Framework

Since CobIT is a worldwide framework which comprises all the international IT standards, including ITIL, CMMI and ISO, current section will commence exploring best practices of service improvement with identifying CobIT's main components and their areas of focus.

CobIT is a business framework dedicated to IT governance, which is used to facilitate business benefits of the company by ensuring that company's resources are responsibly used and all the potential risks are promptly managed. CobIT focuses on Strategic Alignment, Value Delivery, Resource Management, Risk Management and Performance Measurement (CobIT - 4.1, 2017), which is demonstrated by Figure 12 below.

Figure 12. CobIT Focus Areas (rerefence).

As Figure 12 shows, CobIT framework encompasses five focus areas that are responsible for the following processes:

- *Strategic Alignment* of CobIT framework ensures that company's IT infrastructure and functionality comply with the company's objectives and operations.

- *Value Delivery* guarantees that in terms of the company's strategy, 'IT delivers the promised benefits' focusing on the cost optimization (CobIT - 4.1, 2017).

- *Resource Management* is dedicated to optimizing and managing company's IT resources including employees, processes, infrastructure, etc.

- *Risk Management* safeguards the company from all the potential risks by identifying them, informing senior management about them and ensuring that all the determined risks are promptly eliminated by the responsible personnel.

- *Performance Measurement* monitors and analyzes implementation of company's strategy, utilization of the resources and performance of all the processes.

Even though CobIT comprises all the best practices and business frameworks, it is necessary to be equipped with the knowledge about other frameworks that focus on more specific areas of business environment. One of such business frameworks is PRINCE2, which will be described in the next section.

4.2 PRINCE2 Framework

Another widely used method for improving the quality of services is PRINCE2 framework. According to Turley (2013), PRINCE2 comprises the process model of the best practices that can be applied for managing projects.

PRINCE2 framework originated from the United Kingdom where it was initially known as PROMPTII. It appeared in 1975 when Simpact System Ltd. introduced guidelines for project management in response to the situations when multiple IT projects were delayed or exceeded allocated budgets. From 1970s, there have been several revisions of the original project management guidelines and nowadays, PRINCE2 presents the following seven principles, shown in Figure 13, as the basis for successful project management (PRINCE2 2017).

Figure 13. PRINCE2 Principles (PRINCE2 2017).

As can be seen in Figure 13, PRINCE2 encompasses seven main principles: Continued Business Justification; Learn from Experience; Defined Roles and Responsibilities; Manage by Stages; Management by Exception; Focus on Products; Tailor to Suit the Project Environment.

The first and the most important principle of PRINCE2 is defined as *Continued Business Justification* – the process of constant reviewing of a certain project during its life

cycle to justify whether it is beneficial to continue the project or whether it has to be terminated.

The second principal of PRINCE2 is *Learn from Experience* – the process of recording and analyzing already completed projects prior to initiating a new project. The aim of this process is to adjust an active project on the continuous basis according to the identified pitfalls and actions that facilitated success.

The third component of PRINCE2 framework is *Defined Roles and Responsibilities* – the process of ensuring that there is a sufficient amount of employees allocated to the project, and that all the involved parties clearly understand their roles and responsibilities, and capable to fulfill their duties during the whole project. It is especially important when several teams are involved in the project from the customers, supplies and service providers.

Manage by Stages is the fourth principal of PRINCE2 framework. It can be formulated as the process of dividing the project into smaller stages and creating dedicated plan of actions for every stage. This improves control over the project, which consequently ensures continued business justification.

The fifth component of the PRINCE2 infrastructure is *Management by Exception* – the process of executing the project against predefined values of such variables as Time, Scope, Cost, Quality, Benefit and Risk. This eventually enables greater control over the whole project from the managerial point of view.

The sixth, principal of PRINCE2 is *Focus on Products* – the process of creating detailed product or service description, which ensures that customer, supplier and service provider have common understanding about all the features of the product or service.

The last, seventh principal of PRINCE2 framework is *Tailor to Suit the Project Environment* – the process of adjusting the project to the specific needs of any given organization or environment of any specific project. This process provides flexibility and balanced approach towards successful completion of any project.

4.3 ITIL Continual Service Improvement

The other major business framework, which is widely used in the modern IT environment is ITIL3. Since its definition and description of the main elements have been already provided in the current state analysis of the case company, the main focus of further exploration will be on ITIL CSI – Continual Service Improvement phase.

ITIL Continual Service Improvement is the process of providing 'guidance on creating and maintaining value for customers through better strategy, design, transition and operation of services' (ITIL 2012: 256).

ITIL CSI is based on Plan-Do-Check-Act (PDCA) cycle (ITIL 2012: 256), which was developed as a generic method for quality improvement by W. Edwards Deming. Thus, PDCA cycle is also known as Deming cycle. The distinct characteristic of PDCA cycle is that it can be established and used at any stage of the service life cycle for identifying the areas for improvement. Figure 14 below, demonstrates ITIL PDCA cycle (ITIL 2012: 256).

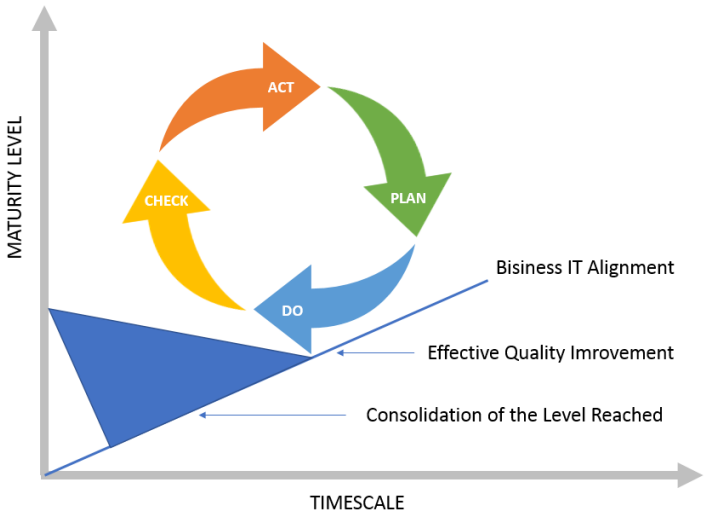


Figure 14. PDCA Cycle (ITIL 2012: 256).

The main purpose of ITIL CSI is to align IT services with the constantly changing business requirements by defining the areas for improvements and implementing necessary improvements to support all the business processes. According to ITIL3 best practices, it can be achieved by performing the following steps: identifying the vision and determining long-term objectives; defining current status and KPIs – Key Performance

Indicators; setting up future objectives and desired KPIs; understanding how to reach future objectives and creating corresponding plan of actions; analysing whether desired objectives and KPIs are met after implementing plan of actions for service improvement; establishing the point at which we have to perform all the previous actions again.

The execution of all the steps described in the previous passage is based on the collected data, which can be acquired according to ITIL CSI recommendations in seven steps: 1) defining the objectives; 2) identifying the subject for measurements; 3) collecting data; 4) processing collected data; 5) analysing collected data; 6) presenting and using the information based on the analysed data; 7) performing improvement.

Taking into consideration the ITIL recommendations concerning seven-step improvement process (ITIL 2012: 276) and PDCA cycle, Continual Service Improvement processes and activities phase can be depicted as shown in Figure 15 below.

Figure 15. The seven-step improvement process (ITIL 2012: 276).

From the practical point of view, ITIL CSI is equipped with the extensive variety of automation and acceleration tools that allow to execute all the tasks of the seven-step improvement process, e.g. Splunk Enterprise which is used for data logging and analysis; Remedy Force which is utilized for advanced reporting and service management; BMC Atrium CMDB which is deployed for configuration management, etc. In addition, ITIL CSI also uses such traditional tools as assessment sheets, surveys, templates, diagrams, scripts, etc.

After analysing the whole set of ITIL CSI tools, it is possible to state that they are all targeted to automate and consequently accelerate all the IT processes. Thus, bearing this in mind, the deeper investigation of the automation phenomenon is introduced in the next chapter.

4.4 Automation as Main Driving Force of ITIL CSI

With the growth of business, any company applies CSI to adjust its processes to the rapidly changing IT environment and these adjustments cannot be efficiently accomplished without automation. It is because automation enables the company to effectively integrate CSI into the daily operations and consequently into the very essence of the company's culture.

The notion of automation first appeared in the automobile industry in 1946 and the 'origin of the word is attributed to D.S. Harder, an engineering manager at the Ford Motor Company at the time (Groover 1999).

Automation can be formulated as a technological process of performing a certain task by means of preprogrammed commands 'combined with automatic feedback control to ensure proper execution of the instructions' (Groover 1999). In other words, automation allows accomplishing certain technological tasks without human assistance. Since automation heavily relies on computer-based technologies, it infiltrated almost all areas of human life, starting from agricultural industry to space industry. Nevertheless, taking into account the scope of the current research, the main focus of further investigation is on automation in the IT industry.

IT automation in comparison with other types of automations, e.g. machinery automation, is purely characterized by the usage of specialized software tools. Another peculiar feature of IT automation is the area of implementation, which can range from automating one specific task to automating the whole process.

IT automation is often affiliated with BPA – Business Process Automation, which is defined by Rouse (2011) as 'the application of IT automation to achieve goals such as increased worker productivity or lower costs of operations'.

According to Rouse (2011), BPA is a subsidiary of IT automation, which is targeted to constantly changing business environment clarifying roles, duties and responsibilities of company's personnel and consequently optimizing operational performance of all processes and resources.

Automation in IT industry is conducted through the extensive usage of various computer-generated platforms, policies, scripts, templates, diagrams, surveys, manuals, etc. They are usually designed in such a way which provides an opportunity for IT administrator to re-use them in different IT environments, e.g. for different UTM platforms.

4.5 Pros and Cons of IT Automation

The benefits of IT automation are undoubtedly invaluable, because it enables employees to omit repetitive tasks and concentrate on the 'tasks that require decision-making and assessment skills' (Rouse 2017). To be more precise, IT automation: increases the speed of completing monotonous task; facilitates accuracy and consistency by eliminating possibility for human errors; ensures flexibility and compatibility in terms of executing the same preprogramed tasks across different IT environments and on different platforms.

It is worth mentioning that IT automation has some minor disadvantages that can cause major issues. It is due to the fact that IT infrastructure of any company undertakes constant changes, but automated processes depend on programed tasks that were once created in the past. Thus, it is of utmost importance to review all the automated processes on a regular basis to avoid propagation of outdated data within company's infrastructure. Alternatively, IT administrators can implement dedicated automated procedures that validate previously created automated tasks.

Another factor that requires urgent attention is the possibility of encoding an error in the automated task or process. In comparison with general human mistakes, errors in the automated process spread very fast within company's infrastructure and cause severe disruptions of various processes. Thus, it is important to allocate dedicated IT administrators who will be responsible purely for automation processes in the company.

The last but not the least thing to be mentioned about automation is that an automated system does not necessarily mean an intelligent system. In this regard, administrators

must educate automated systems to perform certain tasks correctly. It is especially the case with automated AntiSpam policies where valid email messages will end up in the spam folder, and unwanted spam email gets past the filter (Rouse 2017).

4.6 Future of IT Automation

Even though IT automation is not a new concept, it is still undergoing the formation stage, because the amount of new emerging technologies is very vast. In this regard, some practitioners and scholars consider IT automation as the continuous process which entirely depends on human's ability to plan, analyze, encode and implement predefined activities. Other professionals see further development of IT automation mostly in conjunction with AI – Artificial Intelligence, which requires involvement of IT professionals only at the initial stage of creating an automated product or process. They are confident that AI technologies are able to develop, enhance and adjust automated processes by themselves without any human interference.

Nevertheless, irrespective of different views on the subject matter, IT automation will always require assistance from IT professionals. It is because only humans and nobody else are capable to make a decision to what entity automated processes must be applied regardless whether this automated entity is bound to AI or not.

Summing up information about service improvement and IT automation in particular, it is necessary to mention that the concept of IT automation became popular only in the recent decades. The notion of IT automation can be viewed as an umbrella term, because it encompasses automation of all business processes and entities utilizing the best practices and tools for CSI. Hence, the next section only distinguishes those tools of IT automation that can be deployed to address the challenges of the present research.

4.7 Conceptual Framework

After a comprehensive overview of the main aspects of continual service improvement, this research employed the combination of particular service improvement drivers that have been distinguished from the major business management frameworks. The scope of the selected drivers is subject to their adoptability in approaching business challeng-

es defined in the current state analysis. Consequently, the conceptual framework of the current research was created as shown in Figure 16 below.

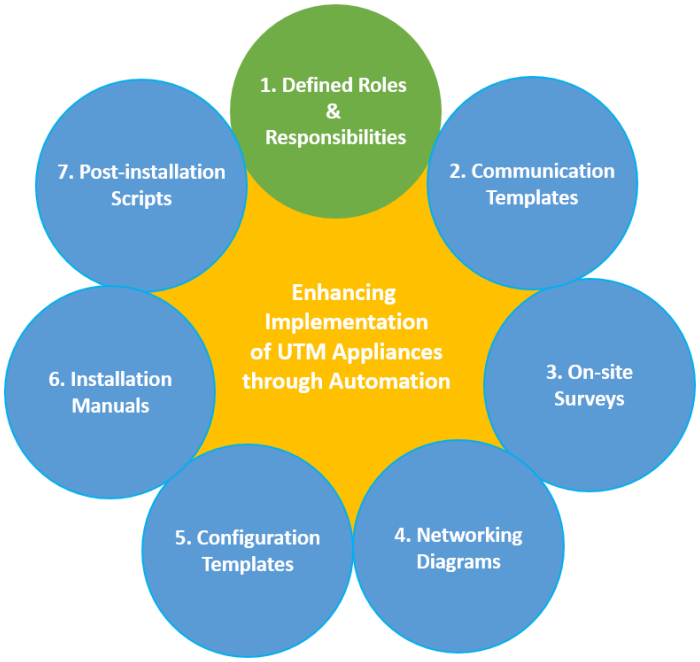


Figure 16. Conceptual Framework.

As Figure 19 demonstrates, the conceptual framework places *automation* in its core as the main driving force for enhancing the implementation process of UTM appliances on the global scale. The main driver, in its turn, encompasses dedicated sub-drivers or tools that facilitate automation of processes on the local scale during various phases of UTM implementation. The first “petal” of the conceptual framework is dedicated to Defined Roles and Responsibilities’ driver, which is intended to be employed to tackle the challenges with *Responsibilities*. The second “petal” of the conceptual framework concerns Communication Templates’ that are going to be used to address the challenges with *Shipment* and partially with *Initial Configuration*. The third, the fourth and the fifth “petals” of the conceptual framework respectively correspond to ‘On-site Surveys’, ‘Networking Diagrams’ and ‘Configuration Templates’ that will be utilized purely in response to the challenges with *Initial Configuration*. The sixth and the seventh “petals” of the conceptual framework are respectively designated to ‘Installation Manuals’ and ‘Post-installation Scripts that will be deployed to deal with *Installation* challenges.

It is important to point out that each automation driver of the conceptual framework is characterized by dedicated action points presented in Table 3 below.

Table 3. Automation Drivers and Associated Action Points.

1. Defined Roles and Responsibilities	
A	Distribution of the roles and responsibilities should be performed in accordance with the objectives and skills of the teams that are involved in a certain project.
B	In order to ensure effective operation of a particular team, it is advisable to monitor its activities and maintain related statistics.
C	It is beneficiary to encourage all the team members to fulfil their duties by conducting weekly review meetings and providing reports about performance of every team member, for example, during one-to-one meetings.
2. Communication Templates	
A	Suppliers of the hardware must precisely know what type of devices they have to deliver. Thus, while ordering a new device, it is necessary to provide as many details as possible concerning desired hardware vendor, model, technical characteristics and related licenses.
B	Concerning technical aspects, it is necessary to communicate to the customers in a clear and concise manner.
C	For the representatives of logistics, it is important to have information about pricing and technical characteristics of the devices in order to ensure their successful delivery to the customers.
3. On-site Surveys	
A	Technical surveys help to determine existing networking infrastructure of the customers, thus facilitating better service concerning service requests, deliveries and incidents.
4. Networking Diagrams	
A	Usage of networking diagrams helps to understand all the peculiarities of the customer's networking infrastructure and consequently provide better service.
B	It is necessary to update existing networking diagrams of the customers on a

	regular basis in order to promptly reflect the changes in their networking infrastructure.
5. Configuration Templates	
A	Configuration templates for configuring external and internal interfaces of the new networking appliances allow to meet various requirements of ISPs – Internet Service Providers.
B	Configuration templates concerning IP routing allow to ensure correct accessibility to the required networking resources in a short period of time.
C	Configuration templates concerning access rights allow to provide access to the networking resources only to authorized users.
D	Configuration templates concerning VPN tunnels, UTM filters and associated firewall policies allow to provide access to the required online resources correctly and efficiently.
E	Up-to-date configuration templates allow services providers to comply with the new requirements of customers' networking infrastructure.
6. Installation Manuals	
A	Generic installation manuals allow even non-technical persons to install new devices and ensure their basic operations.
B	Customer specific installation manuals can be used by the on-site IT personnel to speed up installation of the new devices without any assistance from the supplier.
7. Post-installation Scripts	
A	Scripts can trigger automatic backups.
B	Scripts can be used for enabling automatic upgrades of the outdated firmware.
C	Deployment of specialised scripts cam permit automatic renewal of licenses.

As Table 3 demonstrates, every action point of the automation drivers corresponds to a particular type of guideline or recommendation that serve to enhance the implementation process of UTM devices of the case company. Therefore, gained knowledge about

practical recommendations of automation drivers will be applied to tackle the defined challenges of the implementation process of UTM appliances.

5 Generating Proposal

Incorporating Conceptual Framework and obtained data during the second round of data collection, this section describes the provisional proposal on how to enhance the implementation process of UTM appliances of the case company.

Taking into account that challenges identified during the Current State Analysis introduced considerable obstacles to the whole implementation process of UTM appliances, the provisional proposal included practical recommendations that can be deployed to precisely tackle those particular challenges. Thus, Figure 20 presents a logical scheme of the interrelationships among identified challenges that are specified in Table 2, distinguished drivers of automation and their corresponding actions points or in other words, theoretical guidelines that are specified in Table 3. All the entities of the Figure 17 are encoded in a particular manner, for example:

- C1A, where letter 'C' stands for '*Challenge'* with '*1. Initial Configuration'* concerning '*A. Delivery tickets that do not contain correct and concise information about required configuration for the new UTM appliances'*
- D7A, where letter 'D' stands for *'Driver'* of *'7. Post-installation Scripts'* related to theoretical action point stating that *'Scripts can trigger automatic backups'*, etc.

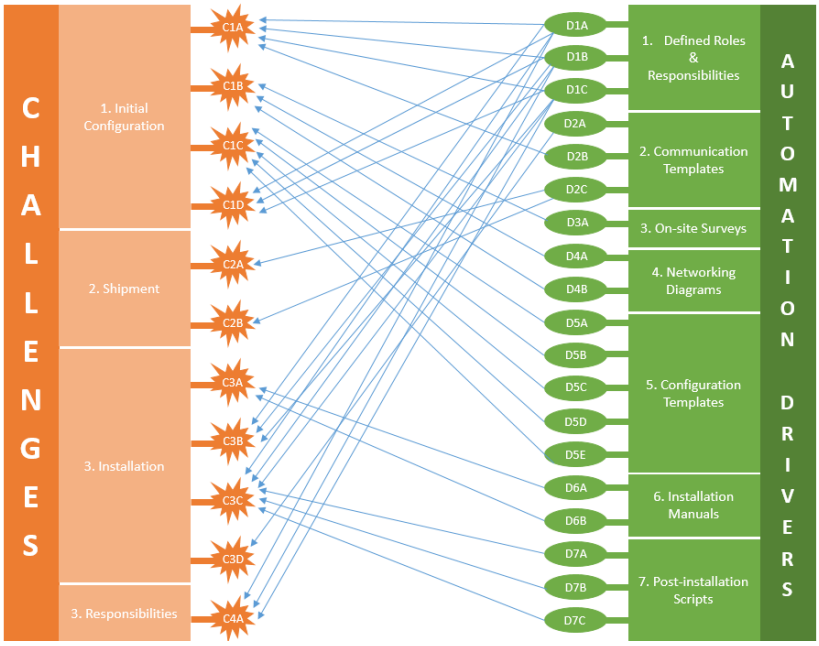


Figure 17. Logical Scheme of the Provisional Proposal.

As Figure 20 demonstrates, each practical instruction of the provisional proposal is based on the theoretical action point of a particular automation driver. And, automation driver in its turn, corresponds to the particular challenge. Hence, this logical construction provides accurate representation of the building blocks of the provisional proposal. In terms of the practical instructions of the provisional proposal, they are shown in Table 4 below.

Table 4. Provisional Proposal.

Provisional Proposal 1: Defined Roles and Responsibilities	
A	To distribute roles and responsibilities among all the teams according to their specialities and objectives.
B	To establish monitoring process in order to verify that all the team members comply with their assigned roles and responsibilities.
C	To conduct weekly review meetings and provide reports to all the team members on how they fulfil their duties.
Provisional Proposal 2: Communication Templates	
A	To create and utilize an e-mail template for communicating with suppliers concerning required hardware and licenses.

B	To create and utilize an e-mail template for communicating with the customers in order to obtain all the required technical details for initial configuration.
C	To create and utilize an e-mail template for communicating with Logistic Department while requesting to send configured devices abroad, especially outside EU.
Provisional Proposal 3: On-site Surveys	
A	To create and use technical surveys (per customer) that will help to determine existing networking infrastructure at any new site of the customer.
Provisional Proposal 4: Networking Diagrams	
A	To create (per customer) networking diagrams of their networking infrastructure based on the initial on-site survey.
B	To keep updated existing networking diagrams of all the customers in order to promptly reflect the changes in their networking infrastructure.
Provisional Proposal 5: Configuration Templates	
A	To create and use generic configuration templates for configuring external and internal interfaces of the new UTM appliances taking into account the type of IP allocation by the local ISP – Internet Service Provider.
B	To create and use (per customer) configuration template concerning preferred network routing
C	To create and use (per customer) configuration template concerning administrative access rights
D	To create and use (per customer) configuration template concerning required VPN tunnels, UTM filters and associated firewall policies.
E	To keep updated all the configuration templates of the customer in order to reflect the changes in their networking infrastructure.
Provisional Proposal 6: Installation Manuals	
A	To create generic installation manual that can be used even by the non-technical person for assisting ENS engineers during the remote installations.

B	To create customer specific installation manual that can be used by the on-site IT personnel to meet customer specific requirements.
Provisional Proposal 7: Post-installation Scripts	
A	To create and deploy (per customer) scripts that enable automatic backups of UTM appliances.
B	To create and deploy (per customer) scripts that enable automatic upgrades of the outdated firmware of UTM appliances.
C	To create and deploy (per customer) scripts that enable automatic renewal of UTM licenses.

As Table 4 demonstrates, practical recommendations of the provisional proposal were built according to the theoretical action points of the specific automation driver. In this regard, it is possible to state that the generated provisional proposal can be employed to tackle previously identified challenges, providing comprehensive collection of tools for enhancing the implementation process of UTM appliances of the case company.

5.1 Validation of Proposal

When the provisional proposal was generated, it was delivered to the internal stakeholder of the case company for validation. Despite the fact that all practical recommendations of the provisional proposal were approved, internal stakeholder made several suggestions.

In regards to *Defined Roles and Responsibilities*, the stakeholder promised to remind the Project Managers to reinforce the awareness of all Delivery Managers about their duties and responsibilities. As for statistics concerning performance of Delivery Managers team (recommendation 1 'B'), it turned out that such statistics exist and the performance of Delivery Managers are evaluated against delivery time and delivery precision values. He also mentioned that these statistics are only available to the head of delivery managers and Project Managers team. Concerning weekly review meetings (recommendation 1 'C'), he suggested that it will be more appropriate to organize them every two weeks or once per month, because of the huge workload that all the teams experience nowadays.

In terms of *Communication Templates* for contacting customers, hardware suppliers and representatives of Logistics Department (recommendations 2 ‘A’, ‘B’, ‘C’), he agreed that they will improve the implementation process of UTM appliances, even though it is a big project which requires considerable investments concerning time and resources.

Regarding *On-site Surveys* (recommendation 3 ‘A’), internal stakeholder admitted that it is important to implement them for all the customers, because at the moment on-site surveys are used for exploring new sites of one customer only.

Concerning *Networking Diagrams*, internal stakeholder is aware that internal database of the case company does not contain any networking diagrams for some of the new customers (recommendation 4 ‘A’) and networking diagrams of the existing customers are out of date (recommendation 4 ‘B’). Thus, he re-confirm the importance of corresponding practical recommendations.

In regards to *Configuration Templates (recommendations 5 ‘A’, ‘B’, ‘C’, ‘D’, ‘E’)*, internal stakeholder mentioned that it is an excellent idea, which will definitely help to eliminate configuration errors and considerably speed up not only initial configuration of the new devices, but the whole implementation process of UTM appliances. Furthermore, he announced that based on the decision of the managerial board, the case company already allocated disk space on the local servers for creating dedicated database of configuration templates per customer.

Concerning *Installation Manuals* (recommendations 6 ‘A’, ‘B’), internal stakeholder greeted this proposal, because installation manuals were used in the past, but nowadays, they are not being used.

As for *Post-installation Scripts*, the internal stakeholder approved the proposals concerning scripts for backups and firmware updates (recommendations 7 ‘A’, ‘B’). As for the scripts related to automatic updates of UTM licenses (recommendation 7 ‘C’), he pointed out that it will be challenging to achieve it, because the extension of UTM licenses depends on the business contracts and must be also coordinated with the vendor, i.e. Fortinet. Thus, the introduction of automatic updates to UTM licenses can cause financial risks, because the system can automatically update UTM licenses on the devices that are no longer supported by the contract or that are about to be termi-

nated. Thus, instead of enabling automatic updates of UTM licenses, he suggested enabling automatic monitoring over all UTM licenses that are purchased the case company. It can be achieved by registering all FortiGate units that are supported by the case company in FortiManager – centralized security management system from Fortinet.

Hence, being armed with recommendations of the internal stakeholder, the provisional proposal was adjusted and is presented in the following section.

5.2 Final Proposal

After scrupulous examination of the remarks of the internal stakeholder, the provisionally proposed recommendations were revised and adjusted, which allowed generating the final proposal presented in Table 5.

Table 5. Final Proposal.

Recommendation 1: Defined Roles and Responsibilities	
A	To remind Delivery Managers about their roles and responsibilities.
B	To enhance existing monitoring process over performance of Delivery Managers.
C	To conduct monthly review meetings and provide reports to all the team members on how they fulfil their duties.
Recommendation 2: Communication Templates	
A	To create and utilize an e-mail template for communicating with suppliers concerning required hardware and licenses.
B	To create and utilize an e-mail template for communicating with the customers in order to obtain all the required technical details for initial configuration.
C	To create and utilize an e-mail template for communicating with Logistic Department while requesting to send configured devices abroad, especially outside EU.
Recommendation 3: On-site Surveys	

A	To create and use technical surveys (per customer) that will help to determine existing networking infrastructure at any new site of the customer.
Recommendation 4: Networking Diagrams	
A	To create (per customer) networking diagrams of their networking infrastructure based on the initial on-site survey.
B	To keep updated existing networking diagrams of all the customers in order to promptly reflect the changes in their networking infrastructure.
Recommendation 5: Configuration Templates	
A	To create and use generic configuration templates for configuring external and internal interfaces of the new UTM appliances taking into account the type of IP allocation by the local ISP – Internet Service Provider.
B	To create and use (per customer) configuration template concerning preferred network routing
C	To create and use (per customer) configuration template concerning administrative access rights
D	To create and use (per customer) configuration template concerning required VPN tunnels, UTM filters and associated firewall policies.
E	To keep updated all the configuration templates of the customer in order to reflect the changes in their networking infrastructure.
Recommendation 6: Installation Manuals	
A	To create generic installation manual that can be used even by the non-technical person for assisting ENS engineers during the remote installations.
B	To create customer specific installation manual that can be used by the on-site IT personnel to meet customer specific requirements.
Recommendation 7: Post-installation Scripts	
A	To create and deploy (per customer) scripts that enable automatic backups of UTM appliances.
B	To create and deploy (per customer) scripts that enable automatic upgrades of

	the outdated firmware of UTM appliances.
C	To register all the FortiGates units in FortiManager in order to enable monitoring over validity of UTM licenses purchased by the case company.

As Table 5 demonstrates, practical recommendations of the final proposal were customized according to the comments of the internal stakeholder to warrant their deployment for enhancing the implementation process of UTM appliances of the case company.

6 Discussion and Conclusions

This section summarizes the current study, evaluates its validity and reliability, and introduces probable development scenarios of the implementation process of UTM appliances within the networking infrastructure of the case company customers.

6.1 Summary

The current research studied how to improve the implementation process of UTM appliances of the case company. The urgency of this improvement was conditioned by the incorrect configuration of UTM appliances, delays with their deliveries to customers' sites and consequently with customer dissatisfaction with Security Gateway services provided by the case company.

Taking into consideration that this situation required immediate cure, the objective of the current research was to identify the strengths and weaknesses in the implementation process of UTM appliances in corporate networks of the customers and eventually produce practical guidelines for Enterprise Network Solutions management team on how to enhance Security Gateway services of the case company.

To carry out this study, *action research* was employed because it is the most applicable research approach for any practitioner who actively observes and analyses any given situation, performs adjustments and modifications to it, and if required moves into completely new direction. To ensure rigorousness, validity and reliability of the current re-

search, its data was obtained from multiple sources during three rounds of data collection.

When business challenges were clarified, related literature sources were analysed to find the remedy that would help to improve the implementation process of UTM appliances of the case company. In regard to the gathered data, it was identified that the most suitable driver for improving the implementation process of UTM appliances turned to be IT automation – one of the Continual Service Improvement drivers of ITIL3 framework.

Then IT automation was examined on a global scale and compared against business challenges identified throughout *current state analysis*. Thus, the most applicable drivers of IT automation that could be utilized to overcome challenges of the current study were identified. As a result, *conceptual framework* of this research was generated.

Furthermore, the second round of data collection was carried out to support the results of the current state analysis. Subsequently, taking into consideration *conceptual framework* and results of the second round of data collection, provisional proposal of the practical guidelines for ENS managerial team was generated.

In the final stage of the research, the company's internal stakeholder was familiarized with the provisional proposal. Eventually, when his feedback was obtained, which comprised the third round of data collection, the final proposal of practical guidelines was generated to meet the objectives of the study.

Summarizing results of the current research, it can be concluded that this study granted the possibility to determine all the strengths and weaknesses of the implementation process of UTM appliances in corporate networks of the case company customers. This information also provided the means of identifying all the challenges in the implementation process of UTM firewalls. To deal with the challenges related to *responsibilities*, the current research recommended to remind all the delivery managers about their duties and to enhance monitoring process over their performance. To tackle the challenges with *initial configuration*, the current research suggested to extensively use configuration templates, communication templates, site surveys and networking diagrams. In terms of challenges with *shipment*, the current research proposed to enhance monitoring over the performance of Delivery Managers and obligatory usage of communica-

tion templates. Concerning challenges with *installation*, the current study urged to create and use installation manuals for the case company customers, thus enabling them to provide basic technical assistance to the ENS engineers during remote installations.

6.2 Managerial Implications

In order to promptly deploy the recommended proposal into the production environment, it is critical to consider managerial implications by allocating necessary activities to the responsible members of the managerial team. Hence, managerial implications related to enhancing the implementation process of UTM appliances through automation are presented in Table 6 below.

Table 6. Managerial Implications.

Activity 1: To improve awareness of Delivery Managers about their roles and responsibilities	
Action Points of Final Proposal: **A, B, C**	Responsible: **Head of the Delivery Management team**
Activity 2: To enhance communication among all the parties involved in the implementation process of UTM appliances	
Action Points of Final Proposal: **A, B, C**	Responsible: **Head of the Delivery Management team and ENS Manager**
Activity 3: To improve exploration of the sites where new UTM appliances are supposed to be installed	
Action Points of Final Proposal: **A**	Responsible: **ENS Manager**
Activity 4: To enhance maintenance of documentation related to networking infrastructures of the case company customers	
Action Points of Final Proposal: **A, B**	Responsible: **ENS Manager**
Activity 5: To improve initial configuration process of UTM appliances	
Action Points of Final Proposal: **A, B, C, D, E**	Responsible: **ENS Manager**
Activity 6: To enhance installation process	
Action Points of Final Proposal: **A, B**	Responsible: **ENS Manager**
Activity 7: To improve post-installation maintenance of the UTM appliances	
Action Points of Final Proposal: **A, B, C**	Responsible: **ENS Manager**

As Table 6 demonstrates, the required activities and related action points are allocated to the dedicated members of the managerial team. Even though the assigned tasks present a considerable workload to the Head of the Delivery Management team and ENS Manager, all these activities require extra time and resources only at the initial state of their implementation. It is due to the fact that as soon as automated procedures are created, they will immediately start brining benefits by releasing resources and providing extra time for more advanced tasks that require analytical thinking and planning. The only fact that must be taken into consideration by the members of the managerial team is that automated system is not an intelligent system. This requires from the members of the managerial team to initiate revising and updating of all automated procedures on a regular basis in order to align them with the constantly changing business environment.

6.3 Evaluation of Validity and Reliability

Considering the previously analysed requirements of the reliable and valid research, the current study produced a valid and reliable outcome. It was gained by conducting three rounds of data collection that facilitated clear understanding of all advantages and disadvantages of the implementation process of UTM appliance; helped to define the challenges and eventually allowed to discover a solution to the research question.

To warrant research validity, the current study exploited qualitative and quantitative research methods. Furthermore, to ensure data triangulation, the study used multiple sources for data collection, e.g. ENS system engineers, external expert, members of the managerial team, internal stakeholder; and different types of data collection techniques, e.g. one-to-one interviews, on-line questionnaires, focus groups, etc.

In terms of replicating the current research, even though the outcome of any research is relatively unique due to such entities as environment, respondents and time, the current study can be effortlessly replicated, because it was conducted in a typical IT environment and because it accommodates a precise description of data collection techniques and analysis.

6.4 Further Development

Due to the nature of IT technologies to introduce changes into the business environment, it is evident that demand for more advanced automated systems will be constantly growing. Hence, there are no doubts that the case company will also thrive to automate certain processes in order to meet all its objectives and consequently gain competitive advantage on the market.

If to reduce the scope of predicting the future of automation to the ENS team and the implementation process of UTM appliances, there will be definitely considerable efforts in producing an extensive library of scripts, templates, diagrams that will eventually improve the configuration, delivery, installation and maintenance of UTM appliances of the case company.

Furthermore, there is a possibility that the case company will start investing into automated systems that are empowered by AI – Artificial Intelligence system, which can be a topic for another research.

References

Tam, K. (2013). UTM security with Fortinet: Mastering FortiOS. SYNGRESS MEDIA.

Case Company Oy (2017). Case Company in brief. [Online] Available at: https://corporate.casecompany.fi/casecompany-in-brief [Accessed on 23 April 2017]

Agutter C. et al (2012). ITIL Foundation Handbook. TSO Information & Publishing Solutions.

CobIT – 4.1 (2017). CobiT-4.1-Brochure. [Online] Available at: http://www.isaca.org/Knowledge-Center/cobit/Documents/CobiT-4.1-Brochure.pdf [Accessed on 25 September 2017]

PRINCE2 (2017). Introduction to PRINCE2. [Online] Available at: https://mplaza.pm/wordpress/wp-content/uploads/2015/11/Introduction-To-PRINCE2-MP0057.pdf [Accessed on 18 October 2017]

Groover, M. (1999). Automation. [Online] Available at: https://www.britannica.com/technology/automation [Accessed on 5 November 2017]

Rouse, M. (2011). Business process automation (BPA). [Online] Available at: http://searchcio.techtarget.com/definition/business-process-automation [Accessed on 25 November 2017]

Rouse, M. (2017). IT Automation. [Online] Available at: http://searchitoperations.techtarget.com/definition/IT-automation [Accessed on 25 November 2017]

Case Company (2017) . Yritysliiketoiminta. [Online] Available at: https://oiva.casecompany.fi/BI/yritysliiketoiminta/Sivut/default.aspx [Accessed on 30 November 2017]

Anand, R. & Vidhyacharan Bhaskar, v. (2012). A unified trust management strategy for content sharing in Peer-to-Peer networks. Department of Electronics and Communication Engineering, SRM University, Kattankulathur 603 203, Tamilnadu, India.

Coughlan, P. and Coghlan, D. (2002). 'Action Research for Operations Management'. *International Journal of Operations & Production Management*, 22 (2): 220-240.

Crume, J. (2000). Inside Internet security: what hackers don't want you to know. Pearson Education Limited.

Forsyth, D. (2010). *Group Dynamics.* 5th Edition. Wadsworth, CENGAGE Learning.

Fortinet Corp. (2012). FortiGate Multi-Threat Security Systems I: Administration, Content Inspection and VPNs. Student Training Guide. Course 201. Fortinet Press.

Fortinet Corp. (2012). FortiGate Multi-Threat Security Systems II: Secured Network Deployment and IPSec VPN. Student Training Guide. Course 301. Fortinet Press.

Giorgia Lodi, G. et al. (2011). An event-based platform for collaborative threats detection and monitoring-Cyber Intelligence and Information Security Research Centre and

Dipartimento di Ingegneria Informatica, Automatica e Gestionale “Antonio Ruberti”, Sapienza University of Rome, Italy.

ISR (2004). International Survey Research. [Online] Available at: www.isrsurveys.com [Accessed on 22 April 2014]

Juanita, E. (2001). The Internet security guide: from planning to deployment. New York: Academic Press.

McNiff, J. (1988). *Action Research: Principles and Practice*. Macmillan Eduction Ltd.

McNiff, J. and Whitehead, J. (2011). *All You Need to Know about Action Research*. 2nd Edition. SAGE Publications Ltd.

Oriyano, S. (2012). Client-side attacks and defense. Syngpress. 225 Wyman Stree, Waltham, MA 02451, USA.

Oxford Advanced Learner’s Dictionary (1997). 5th Edition. Oxford: Oxford University Press.

Stevens, M. 2006). UTM: one-stop protection. Network Security. Volume 2006, Issue 2. P. 12–14.

Swetnam, D. (2004). *Writing your Dissertation: The bestselling guide to planning, preparing and presenting first-class work.* 3rd Edition. How to Books Ltd.

Thorsten Kurpjuhn, T. (2013). The evolving role of the UTM appliance. Network Security. Volume 2013, Issue 1. ZyXEL Communications. p. 8-11.

Vacca, J. (2007). Practical internet security. New York, NY: Springer.

Yin, R. (2003). *Case study research: Design and methods.* Thousand Oaks, CA: Sage. 3rd Edition.

Appendix 1. One-to-one Interview

Question:

'From your own perspective, what factors could simplify and make more effective implementation process of UTM appliances in the networking infrastructure of customers?'

Answers of Respondent: 'A'
I think, we would be able to process deliveries more efficiently, if customers provided precise information about what they actually want. Customers must blankly say I want to configure this firewall with the local breakout to the Internet for accessing external resources and with the IPSec VPN tunnel for accessing internal resources.
It would be nice if Delivery Managers make sure that we have all the information about IP addresses for configuring internal and external side of the firewall, because nowadays we have to get this information form the customer. As far as you know, sometimes it is quite difficult to get it.
I believe that if we had exact physical address and contact details of the local person, we would organise shipping much faster. Instead, of dealing with our direct tasks, we have to get this information from the customer.
Delivery Managers must make sure that all the firewalls that they bought have valid UTM licenses, because we receive more and more complaints from the customers. You could see that on some new firewalls UTM filters are not enabled, even though customers pay for this.
It would be nice to have some kind of standard configuration for all the customers or at least, standard configuration per customer, because we cannot use FortiManager.
It would be excellent if we could install firewall during our working hours or at least, early in the morning, because it is a nightmare to stay after working day and spent two or 3 hours with the local person who does not know what he is doing.
It would be great to deal with the local person who is more or less understand in networking, because it takes ages to do a simple task, e.g. to connect to the firewall via FortiExplorer and provide remote access via TeamViewer.
It would be good if our Delivery Managers could allocated Delivery Tickets taking into account the workload of every ENS engineer.

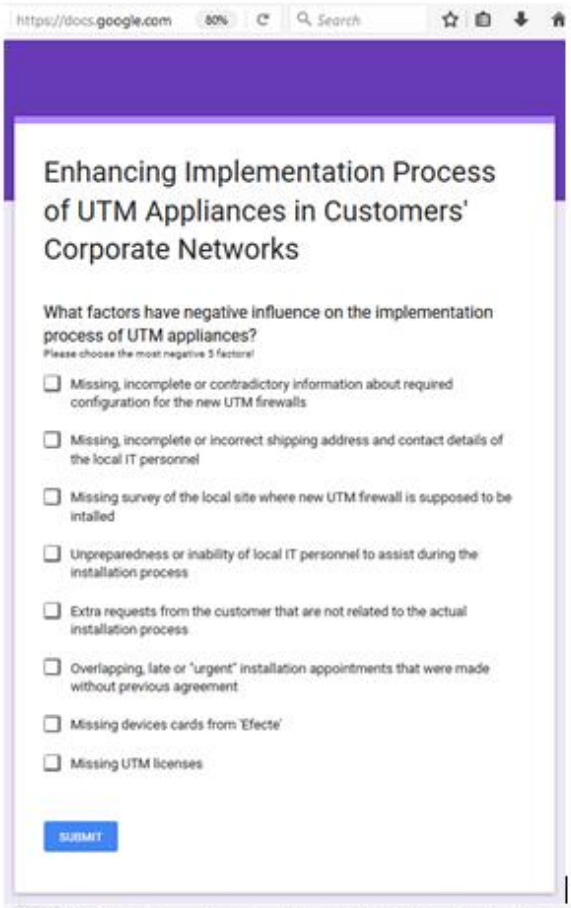
Answers of Respondent: 'B'
Exact information about IP addresses for 'WAN1' and 'internal' interfaces, DHCP, DNS, etc.
Correct information about shipping address, e-mail and mobile phone of the local IT support.
Every delivery should have device card, so we would not waste our time asking Delivery Managers to create it.
Our Technical Account Managers or Customer Relations Managers, or whoever is responsible for this, should explain to the customers the difference between installation and additional service requests, because during installation customers try to build tunnels to all the possible and impossible sites, to shape the traffic, to enable load balancing, etc. You know that it is not part of our standard service.
During installation, I want to speak to the guy who understands either Finnish or English, because sometimes you cannot just understand local person at all.
I think, we have to create some sort of instructions to the local IT guys so they would know how to connect the firewalls, because some of them plug in ISP cable in the 'internal' interface of the firewall.
Local IT guys must have local administrative rights on their PCs, otherwise we cannot just connect remotely to our devices.
We must restrict installation only to the scheduled time.
Customers should make installation appointments well in advance and not like informing you 1 hour before installation, or saying: "I want to do it now!"

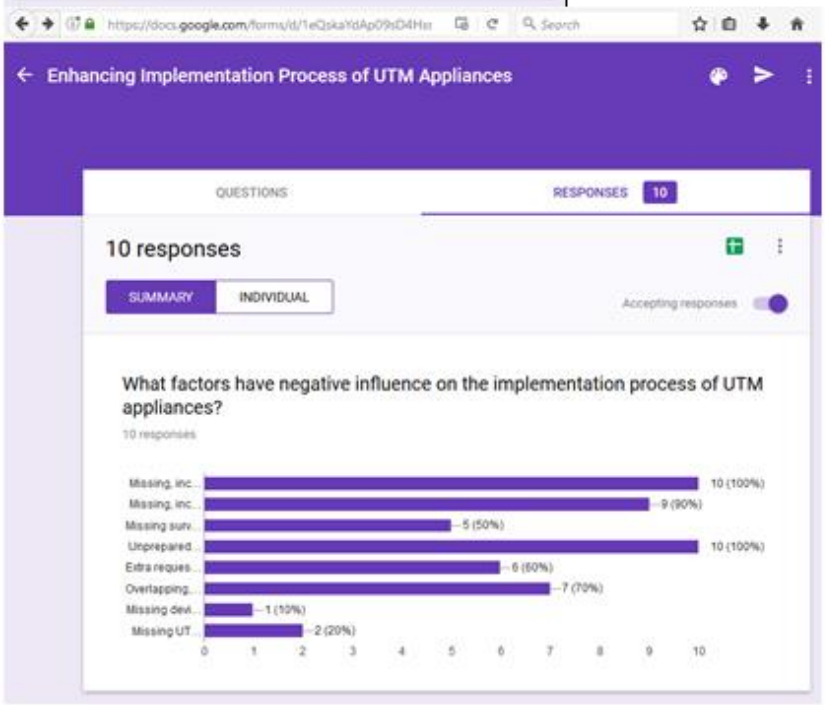
Answers of Respondent: 'C'
Delivery Ticket must have Efecte device card for the new device.
It should be customer's responsibility or responsibility of the Delivery Manager to make sure that Delivery Ticket has all the contact details for shipment.
Configuration details must be uploaded to the Delivery Ticket in advance.
If we help to install firewall outside normal working hours, there must be some special fees for this service.
We might need to create instructions for local IT guys how to help us to get connected to the firewall remotely if we need to do so.
We should not be taking care about licensing staff. Delivery Managers must do it.
It would be great to have some kind of bonus if we process deliveries according to SLA.

Answers of Respondent: 'D'
Customers must stick to the original plan of configuration, which was initially submitted to us. They should not change everything on the fly.
Delivery Managers must make sure that Delivery Ticket has correct info about IP addressing and shipment.
All our guys must record info about IP address, admin credentials, etc. of the new firewall in Efecte, because if somebody from our team will get sick and you "win" to take care about his delivery, you do not even know how to access the firewall. It is quite embarrassing when customer realizes what is going on.
Customers must be informed that during installation we only install the firewall and make sure that local users have access to the Internet and internal resources via IPSec VPN. If they want to do anything extra, they must do it via a separate 'Service Request' tickets or they should be charged somehow.
I do not mind to assign UTM licenses to the new firewall myself, but Delivery Managers or the person who is responsible for purchasing and updating the licenses must give us contract number that we can use to activate those licenses.
It is cool when local IT fellow prepares everything for our installation session.

Answers of Respondent: 'E'
It would be great to have some kind of 'check list' about what information we need from the customer and what information customer should provide to us.
It would be good to have access to repository of licensing contracts so we could activate UTM licenses ourselves.
It would be nice if local IT guys, could send us pictures that would show what devices they have at the local site, so we would have clear picture how to connect our firewall.
It would be also helpful if local IT guys could provide temporary access to ISP router so we would be able to adjust the settings and make sure that our firewall is not blocked on the ISP device.
It is great when customer can confirm if new firewall should be configured with the dynamic IP allocation for the external side or with the static one.
It would be nice if local IT person at customer's site would be somehow guided or trained what to do in order to assist us.
It would be awesome if strictly defined duties and responsibilities of the delivery managers and ENS engineers.
It could be nice if Delivery Managers would be more considerate when they are making installation appointments with the customers, especially for the locations that have time difference with Finland.

Appendix 2. Web-based Questionnaire





Appendix 3. Focus Group

From the perspective of your department, please provide comments on what Enterprise Network Solutions engineers could:	
Question:	**Include in their practices, because it would improve implementation process of UTM appliances?**
Answers:	They could be more proactive in terms of contacting the customer, if they notice that a certain delivery does not have information about configuration details for the new UTM firewall, details of the local support person or shipment details. They could be more responsible with updating the status of the delivery ticket , because if they fail to update the status of already completed delivery, the financial department will fail to invoice the customer on time. They could be more attentive concerning UTM licenses, in oder to avoid situations when UTM deivces are implemented, but UTM licenses are not active.
Question:	**Preserve in their practices, because it positively influences implementation process of UTM appliances?**
Answers:	Excellent customer services skills while communicating with the customers during installation process. Availability to assist the customer with installation process at any time on customer's convenience. High level of technical expertise to meet different requirements of customers during the installation. Ability to provide customers with the technical advice during configuration and installation stages.
Question:	**Exclude from their preactices, because it negatively influences implementation process of UTM appliances?**
Answers:	They could stop themselves from being involved in implementing non-standard UTM services and spending resources in non-productive manner. They must stop completing additional customer's requests through the same Delivery Ticket.

Appendix 4. Interview with External Expert

Question: What facstors have positive impact on the implementation process of UTM appliances within networking environment of your customers?

Answers:

1) Before shipping new device to the customer, we are trying to obtain precise information about required configuration

2) We are trying to avoid installations, when customer encourages us to send the device without any configuration and configure it on the fly upon the delivery

3) We encourage our engineers to automate the process of configuring new devices by maintaining pieces of code that are usually implemented on all our devices, e.g. SNMP configuration related to our monitoring system.

4) We provide our customers with instrucstions on how to connect the devices at their local sites.

5) We are trying to make installation appointments at the time which is suitable for our customers and also for our engineers. Especially, it is related to installations in the countries that have time difference with Finland.

6) We encourage, our engineers to schedule installaton appointments well in advance so they could spend their time and efforts more efficiently, and avoid situations when customer inclined to turn our engineer into a "personal IT servant", who can be contacted at any time during day and night.

7) We ensure that in case of emergency, our dedicated support engineer has a peer colleague who can serve as a back up during installation phase

8) We provide constant internal and external trainings for our engineers to ensure that they can meet requirement of our customers in terms of the new technologies and services.

9) We inspire our engineers for continious learing and development of their professional skills.

10) Depending on customer's SLA, we provide possiblity for our customers to install new UTM devices outside normal working hours, which is subject to extra charges.